Colorado Department of
Health Care Policy and Financing

PBMS Contract

STATE OF COLORADO
Department of Health Care Policy and Financing Contract with Magellan Medicaid Administration, Inc. for the PBMS and Services
TABLE OF CONTENTS

1. PARTIES

This Contract (hereinafter called "Contract") is entered into by and between Magellan Medicaid Administration, Inc., 11013 W. Broad Street, Suite 500, Glen Allen, VA 23060 (hereinafter called "Contractor"), and the STATE OF COLORADO acting by and through the Department of Health Care Policy and Financing, 1570 Grant Street, Denver, Colorado 80203 (hereinafter called the "State" or "Department"). Contractor and the State hereby agree to the following terms and conditions.

2. EFFECTIVE DATE AND NOTICE OF NONLIABILITY

This Contract shall not be effective or enforceable until it is approved and signed by the Colorado State Controller or designee (hereinafter called the "Effective Date"). The State shall not be liable to pay or reimburse Contractor for any performance hereunder including, but not limited to, costs or expenses incurred, or be bound by any provision hereof prior to the Effective Date.

3. RECITALS

A. Authority, Appropriation, and Approval
Authority to enter into this Contract exists in CRS 25.5-1-101 *et seq*., and funds have been budgeted, appropriated and otherwise made available and a sufficient unencumbered balance thereof remains available for payment. Required approvals, clearance and coordination have been accomplished from and with appropriate agencies.

B. Consideration
The Parties acknowledge that the mutual promises and covenants contained herein and other good and valuable consideration are sufficient and adequate to support this Contract.

C. Purpose
The purpose of this Contract is to develop and install the Pharmacy Benefits Management System (PBMS), as defined below, and provide the Services, as defined below and as set forth in this Contract, including all Attachments and Exhibits. Contractor's offer, submitted in response to Request for Proposal Number HCPFRFPKC13PBMS was selected by the State.

D. References
All references in this Contract to sections (whether spelled out or using the § symbol), subsections, exhibits or other attachments, are references to sections, subsections, exhibits or other attachments contained herein or incorporated as a part hereof, unless otherwise noted.

4. DEFINITIONS

The following terms when capitalized as used herein shall be construed and interpreted as follows:

A. "Abandon" and "Abandonment" shall have the meaning set forth in **§15.A.v**.

B. "Addendum" shall have the meaning set forth in **§10.B**.

C. "Business Day" regardless of whether capitalized or not, means any day in which the Department is open and conducting business. Business Days shall not include weekend days or any day on which the Department observes one of the following holidays:

i. New Year's Day.

ii. Washington-Lincoln Day (also referred to as President's Day).

iii. Memorial Day.

iv. Independence Day.

v. Labor Day.

vi. Thanksgiving Day.

vii. Christmas Day.

D. "Contract" means this agreement, its terms and conditions, and including all attached addenda, exhibits, documents incorporated by reference under the terms of this agreement, and any future modifying agreements, exhibits, attachments or references incorporated herein pursuant to this agreement, Colorado State law, Fiscal Rules, and State Controller Policies.

E. "Contract Funds" means funds available for payment by the State to Contractor pursuant to this Contract.

F. "Contractor Property" shall have the meaning set forth in **§17.A**.

G. "Days" regardless of whether capitalized or not, means Business Days unless otherwise specified.

H. "Defect" shall mean an error, flaw, mistake, failure, or fault in a computer program or system that produces an incorrect or unexpected result that differs from an agreed-to Specification, or causes it to behave in unintended ways that differ from an agreed-to Specification.

I. "Disabling Code" shall have the meaning set forth in **§12.F.**

J. Exhibits and other Attachments. The following documents are attached hereto and incorporated by reference herein:

HIPAA Business Associate Addendum and Attachment A

Exhibit A, Statement of Work

Exhibit B, Sample Option Letter

Exhibit C, Requirements

Exhibit D, Project Phase Document

Exhibit E, Compensation and Quality Maintenance Payments

Exhibit F, Terminology

Exhibit G, Performance Standards

Exhibit H, State Cybersecurity Policies

K. "Goods" means tangible material acquired, produced, or delivered by Contractor either separately or in conjunction with the Services Contractor renders hereunder.

L. "HIPAA" shall have the meaning set forth in **§10.B.**

M. "Including" or "includes", regardless of whether capitalized or not, means "including, without limitation".

N. "MMIS" means the Department's automated mechanized claims processing and information retrieval system for Medicaid. In conjunction with this Contract, the Department has also contracted with HP Enterprise Services to develop a new MMIS named Colorado interChange, and the term MMIS shall include this new system.

O. "Operational Start Date" is defined in **Exhibit F**, Terminology, as the date on which the Department authorizes Contractor to begin the PBMS Ongoing Operations and Enhancement Contract Stage.

P. "Party" means the State or Contractor and Parties means both the State and Contractor.

Q. "PBMS" means a system to meet specific requirements of the State to provide pharmacy benefit management services as specified under this Contract.

R. "PBMS Ongoing Operations and Enhancement Contract Stage" is defined in **Exhibit A**, Statement of Work.

S. "Quarterly Milestones" will be as identified in **Exhibit A**, Compensation and Quality Maintenance Payments.

T. "Record Retention Period" shall have the meaning set forth in **§9.A**.

U. "Review" means examining Contractor's Work to ensure that it is adequate, accurate, correct, and consistent with the provided Specifications, if any, and in accordance with the standards described in this Contract.

V. "Services" means the required services to be performed by Contractor pursuant to this Contract.

W. "Software And Data" means software, source code, information and data in any form and fixed or stored in any manner.

X. "State Fiscal Year" or "SFY" means the period which begins on July 1 of each calendar year and ends on June 30 of the following calendar year.

Y. "State Property" shall have the meaning set forth in **§17.A**.

Z. "Subcontractor" means third-parties, if any, engaged by Contractor to undertake the performance of a portion of its obligations.

AA. "Third Party Property" shall have the meaning set forth in **§17.C**.

BB. "Third Party Users" means persons or entities with whom the State contracts, other than the Parties, to use or provide services in connection with the PBMS.

CC. "Work" means the tasks and activities Contractor is required to perform to fulfill its obligations under this Contract, including the performance of the Services and delivery of the Goods.

DD. "Work Product" means the tangible or intangible results of Contractor's Work, including, but not limited to, deliverables, software (including all computer code, firmware, internal code, microcode and other forms of code, in any form), research, reports, studies, data, photographs, negatives or other finished or unfinished documents, drawings, models, surveys, maps, materials, or work product of any type, including drafts.

Any terms used herein which are defined in the Exhibits shall be construed and interpreted as defined therein.

5. TERM

A. Initial Term

The Parties' respective performances under this Contract shall commence on the Effective Date. This Contract shall expire on October 31, 2020, unless sooner terminated or further extended as specified elsewhere herein.

B. Two Month Extension

The State, at its sole discretion, upon written notice to Contractor as provided in **§16**, may unilaterally extend the term of this Contract for a period not to exceed two (2) months if the Parties are negotiating a replacement contract at or near the end of any initial term or renewal term. The provisions of this Contract in effect when such notice is given, including, but not limited to, prices, rates and delivery requirements, shall remain in effect during the two month extension. The two (2) month extension shall immediately terminate when and if a replacement contract is approved and signed by the Colorado State Controller or an authorized designee.

C. First Option to Extend

The State may require continued performance for up to three (3) additional years starting on November 1, 2020 and ending no later than October 31, 2023 at the same rates and same terms specified in the Contract. If the State exercises this option, it shall provide written notice to Contractor at least thirty (30) days prior to the end of the current Contract term in form substantially equivalent to **Exhibit B, Sample Option Letter**. If exercised, the provisions of the Option Letter shall become part of and be incorporated into this Contract.

D. Second Option to Extend

Subject to approval of CMS and requisite State approvals, the State may request continued performance for up to two (2) additional years starting on November 1, 2023 and ending no later than October 31, 2025 at mutually agreed rates and on the same terms specified in this Contract. If the State exercises this option, it shall provide written notice to Contractor at least thirty (30) days prior to the end of the current Contract term in form substantially equivalent to **Exhibit B, Sample Option Letter**. If exercised, the provisions of the Option Letter shall become part of and be incorporated into this Contract.

Any agreed increase in rates under this Section 5.D shall be limited as follows:
In no event will the rates agreed under this Section 5.D exceed the rates covering the period from November 1, 2022 to October 31, 2023 as specified in this Contract plus a maximum percentage increase equal to the mathematical mean of the annual percent increase in the Consumer Price Index for All Urban Consumers (CPI-U) for the Denver-Boulder-Greeley metropolitan area for calendar year 2019 and calendar year 2020 as published by the US Department of Labor, Bureau of Labor Statistics. If the CPI-U is for some reason not available as specified in this Section, the Parties will use the CPI-U (U.S.) for the same period.

6. STATEMENT OF WORK

A. Completion

Contractor shall complete the Work and its other obligations as described in this Contract, on or before the end of the term of this Contract. The State shall not be liable to compensate Contractor for any Work performed prior to the Effective Date or after the expiration or termination of this Contract.

B. Goods and Services

Contractor shall procure Goods and Services necessary to complete the Work. Such procurement shall not increase the maximum amount payable hereunder by the State.

C. Independent Contractor

All persons employed by Contractor or Subcontractors to perform Work under this Contract shall be Contractor's or Subcontractors' employee(s) for all purposes hereunder and shall not be employees of the State for any purpose as a result of this Contract.

D. Performance

Contractor will provide Design, Development and Implementation of the PBMS and perform Services as described in this Contract.

E. Operational Start Date

The Operational Start Date is established through the Project Management Plan, as described in **Exhibit C**, Requirements. The Operational Start Date may be changed by the Parties as mutually agreed through a modification to the Project Management Plan.

7. PAYMENTS TO CONTRACTOR

The State shall, in accordance with the provisions of this **§7** and **Exhibit E**, Compensation and Quality Maintenance Payments, and the State's receipt of a correct invoice and the State's exercise of their remedies as provided in this Contract, pay Contractor in the amounts and using the methods set forth below:

A. Maximum Amount

The maximum amount payable under this Contract to Contractor by the State is shown in the following table, as determined by the State from available funds. Payments to Contractor are limited to the unpaid obligated balance of the Contract at the rates set forth in **Exhibit E,** Compensation and Quality Maintenance Payments. The maximum amount payable by the State to Contractor is:

State Fiscal Year 2015-16	$4,909,615.35
State Fiscal Year 2016-17	$4,940,384.65
State Fiscal Year 2017-18	$2,925,000.00
State Fiscal Year 2018-19	$2,925,000.00
State Fiscal Year 2019-20	$2,925,000.00
State Fiscal Year 2020-21	$2,925,000.00
State Fiscal Year 2021-22	$2,925,000.00
State Fiscal Year 2022-23	$2,925,000.00
State Fiscal Year 2023-24	$925,000.00
Total for All State Fiscal Years	**$28,325,000.00**

The State Fiscal Year amounts in the table in this section are based on State appropriations. Based on the timing of the invoicing and payment, the Contractor may receive amounts paid in a different State Fiscal Year than when the amounts were actually earned by the Contractor.

Any changes to the maximum amount payable under the Contract or Quality

Maintenance Payments Specified in Exhibit E, shall require a formal written amendment, in accordance with State Fiscal Rules and State Controller Policies and Guidelines

B. Payment

Payment pursuant to this Contract will be made as earned pursuant to the terms of this Contract. Any advance payments allowed under this Contract shall comply with State Fiscal Rules and be made in accordance with the provisions of this Contract. Contractor shall initiate any payment requests by submitting invoices to the State in the form and manner prescribed by the State. The State shall notify Contractor within 30 days of receipt of the invoice related to any dispute. Invoice disputes shall follow the Dispute Process in § 20.E. The State shall fully pay each invoice within 45 days of receipt thereof if the invoice represents performance by Contractor previously accepted by the State, subject to the limitations set forth in this Section.

C. Interest

Uncontested amounts not paid by the State within 45 days shall bear interest on the unpaid balance beginning on the 46th day at a rate not to exceed one percent per month until paid in full, provided, however, that interest shall not accrue on unpaid amounts that are subject to a good faith dispute. Contractor shall invoice the State separately for accrued interest on delinquent amounts. The billing shall reference the delinquent payment, the number of day's interest to be paid and the interest rate.

D. Available Funds-Contingency-Termination

The State is prohibited by law from making commitments beyond the term of the State's current Fiscal Year. Therefore, Contractor's compensation beyond the State's current Fiscal Year is contingent upon the continuing availability of State appropriations as provided in the Colorado Special Provisions, set forth below. If federal funds are used to fund this Contract, in whole or in part, the State's performance hereunder is contingent upon the continuing availability of such funds. Payments pursuant to this Contract shall be made only from available funds encumbered for this Contract and the State's liability for such payments shall be limited to the amount remaining of such encumbered funds. If State or federal funds are not appropriated, or otherwise become unavailable to fund this Contract, the State may terminate this Contract by notice, with as much notice as reasonably possible, in whole or in part, without further liability notwithstanding any notice and cure period in **§14.B**. If the Contract is terminated for lack of appropriation, the termination date cannot extend beyond the period of the then current appropriation and the amount payable cannot exceed the existing appropriated funds.

E. Erroneous Payments

At the State's sole discretion, payments made to Contractor in error for any reason, including, but not limited to, overpayments or improper payments, may be recovered from Contractor by deduction from subsequent payments under this Contract or other contracts, grants or agreements between the State and Contractor or by other appropriate methods and collected as a debt due to the State. Such funds shall not be paid to any party other than the State.

F. Closeout Payments

Notwithstanding anything to the contrary in this Contract, all payments for the final month of the Contract shall be paid to Contractor no sooner than ten (10) days

after the Department has determined that Contractor has completed all of the requirements of the Turnover Phase, as defined in Exhibit D, Project Phase Document.

G. Recoupment of erroneous payments

All payments, adjustments, and other financial transactions made through the PBMS will be made on behalf of eligible members to active Enrolled Providers for approved services and in accordance with the payment rules. Contractor shall be liable for the actual amount of all detected erroneous payments identified as a result of State or Federal claims reviews or as reported by Providers or from other referrals that are a result of Contractor (i) staff action, (ii) inaccurate system data, (iii) inaccurate processing or (iv) PBMS malfunction. Such liabilities may be withheld from Contractor payments. Contractor, however, shall have the right to seek recovery on behalf of the State from Providers to whom erroneous payments are made using voluntary refund, offset recovery, or other State-approved methods. Contractor shall notify the State promptly upon discovery of any erroneous payments, irrespective of cause, and prior to initiating appropriate recovery action. The State shall provide support necessary for the Contractor to make any recoupments under this section.

Contractor must pay to the State any portion of an erroneous payment not recouped within one-hundred and eighty (180) calendar days of its receipt of the direction initiating its recoupment. Contractor will make such payment to the State within seven (7) calendar days of the expiration of the one-hundred and eighty (180) calendar-day timeframe. The State shall not be liable to Contractor for any erroneous payment due that is not recovered by recoupment from Providers. Contractor may initiate independent recovery procedures and actions once the recoupment process described herein has been completed and a repayment amount remains outstanding. The State may review proposed independent recovery procedures. If the State recovers any erroneous payments for which Contractor has reimbursed the State, the State shall notify Contractor, who shall then submit an invoice for the returned amount.

H. Option to Increase or Decrease Statewide Quantity of Service

If the actual volume of claims/Encounters increases by greater than twenty percent (20%) from the forecasted claims/Encounters estimate provided in **Exhibit A**, Statement of Work, Contractor may request a change to the Contract pricing or decreases in service level or scope, but the Department does not guarantee that funding will be available to increase the Contract price or that it will amend the Contract to meet Contractor's request. Any increase in the Contract price may require a formal budget action that must be approved by the Department and the Colorado General Assembly, so there is no guarantee that the Contract price will increase for any reason, including those outside the control of Contractor. Any dispute with regard to the appropriate remedy or change in Contract price will be resolved through the Dispute Process in **§20.E.**

I. Change in Circumstance; Modification

In the event that the Contractor reasonably believes that a change in a law, regulation, how Medicaid is administered by the State or other change in circumstance, that cannot be addressed through the Change Management Process or Section 7.H above, will significantly interfere with the Contractor's ability to perform in compliance with

this Contract, then the Contractor may submit a request to the Department to modify the Contract price, service level or scope to account for that change. If the request is approved, the Department does not guarantee that funding will be available to increase the Contract price or amend the Contract to meet Contractor's request. Any increase in the Contract price may require a formal budget action that must be approved by the Department and the Colorado General Assembly, so there is no guarantee that the Contract price will increase for any reason, including those outside the control of Contractor.

8. REPORTING NOTIFICATION

Reports required under this Contract shall be in accordance with the procedures and in such form as prescribed by the State and as described in **Exhibit C**, Requirements and the Communication Management Plan.

A. Litigation Reporting

Within twenty (20) days after being served with any pleading in a legal action filed with a court or administrative agency that is directly related to this Contract or which may directly affect Contractor's ability to perform its obligations hereunder, Contractor shall notify the State of such action and deliver copies of such pleadings to the State's principal representative as identified herein to the extent not prohibited by law. If the State's principal representative is not then serving, such notice and copies shall be delivered to the Executive Director of the Department.

B. Noncompliance

Contractor's failure to provide reports and notify the State in a timely manner in accordance with this **§8** may result in the delay of payment of funds and/or termination as provided under this Contract.

9. CONTRACTOR RECORDS

A. Maintenance

Contractor shall make, keep, maintain, and allow inspection and monitoring by the State of a complete file of all records, documents, communications, notes, and other written materials, electronic media files and electronic communications, pertaining in any manner to the Work or the delivery of Services or Goods hereunder in order to verify the accuracy of Contractor's invoices and shall not include Contractor's internal books and records. Contractor shall maintain such records until the last to occur of: (i) a period of six (6) years after the date this Contract expires or is sooner terminated, or (ii) a period of six (6) years after final payment is made hereunder, or (iii) a period of six (6) years after the resolution of any pending Contract matters, or (iv) if an audit is occurring, or Contractor has received notice that an audit is pending, until such audit has been completed and its findings have been resolved (collectively, the "Record Retention Period"). All such records, documents, communications and other materials shall be the property of the State, and shall be maintained by Contractor in a central location and Contractor shall be custodian on behalf of the State.

B. Inspection

Contractor shall permit the State, the federal government and any other duly authorized agent of a governmental agency to audit, inspect, examine, excerpt, copy

and/or transcribe Contractor's records related to this Contract during the Record Retention Period, to assure compliance with the terms hereof or to evaluate performance hereunder or to verify the accuracy of Contractor's invoices. The State reserves the right to inspect the Work with reasonable notice and at all reasonable times and places during the term of this Contract, including any extensions or renewals. If the Work fails to conform to the requirements of this Contract, the State may require Contractor promptly to bring the Work into conformity with Contract requirements, at Contractor's sole expense. If the Work cannot be brought into conformance by re-performance or other corrective measures, the State may require Contractor to take necessary action to ensure that future performance conforms to Contract requirements and exercise the remedies available under this Contract, at law or in equity, in lieu of or in conjunction with such corrective measures.

C. Monitoring

Contractor shall permit the State, the federal government and any other duly authorized agent of a government agency, in their sole discretion, to reasonably monitor all activities conducted by Contractor pursuant to the terms of this Contract using any reasonable procedure, including, but not limited to: internal evaluation procedures, examination of program data, formal audit examinations, or any other procedure, provided that such procedures do not unreasonably interfere with Contractor's performance hereunder and are not unreasonably burdensome as to frequency, scope and duration. The State shall provide Contractor at least five (5) Business Days written notice prior to any such monitoring.

D. Final Audit Report

If an audit is performed by any governmental agency on Contractor's records for any Fiscal Year covering a portion of the term of this Contract, Contractor shall submit a copy of the final audit report to the State or its principal representative at the address specified herein.

10. CONFIDENTIAL INFORMATION

Contractor shall comply with, and shall cause each of its Subcontractors and any other party performing work under this Contract to comply with the provisions of this **§10** if it becomes privy to Confidential Information in connection with its performance hereunder. "Confidential Information" means all information provided or made available to Contractor by the State or its agents or employees that is marked or otherwise identified as confidential or proprietary or which Contractor knows or reasonably should know is confidential or proprietary information. Confidential Information also includes all State records, personnel records and information concerning individuals and all other information subject to confidentiality obligations set forth in **§10.B** below. Such information shall not include information required to be disclosed pursuant to the Colorado Open Records Act, CRS §24-72-201, *et seq.*

A. Confidentiality

Contractor shall keep all Confidential Information confidential at all times and comply with all laws and regulations concerning confidentiality of information. Any request or demand by a third party for State records and information in the possession of Contractor shall be immediately forwarded to the State's principal representative.

B. Health Insurance Portability & Accountability Act of 1996 ("HIPAA")

i. Federal Law and Regulations

Pursuant to federal law and regulations governing the privacy of certain health information, Contractor, to the extent applicable, shall comply with the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §1320d – 1320d-8 ("HIPAA") and its implementing regulations promulgated by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 (the "Privacy Rule") and other applicable laws, as amended.

ii. Business Associate Contract

Federal law and regulations governing the privacy of certain health information requires a "Business Associate Contract" between the State and Contractor, 45 C.F.R. Section 164.504(e). Attached and incorporated herein by reference and agreed to by the parties is a HIPAA Business Associate Addendum ("Addendum") for HIPAA compliance. Terms of the Addendum shall be considered binding upon execution of this Contract and shall remain in effect during the term of the Contract including any extensions or amendments.

iii. Confidentiality of Records

Contractor shall protect the confidentiality of all records and other materials containing personally identifying information that are maintained in accordance with the Contract and comply with HIPAA rules and regulations. Except as provided by law, no information in possession of Contractor about any individual constituent shall be disclosed in a form including identifying information without the prior written consent of the person in interest, a minor's parent, or guardian. Contractor shall have written policies governing access to, duplication and dissemination of, all such information. Contractor shall advise its employees, agents and subcontractors, if any, that they are subject to these confidentiality requirements. Contractor shall provide its employees, agents and subcontractors, if any, with a copy or written explanation of these confidentiality requirements before access to confidential data is permitted. No confidentiality requirements contained in this Contract shall negate or supersede the provisions of HIPAA.

C. Notification

Contractor shall notify its agents, employees, Subcontractors and assigns who may come into contact with State records or other Confidential Information that each is subject to the confidentiality requirements set forth herein, and shall provide each with a written explanation of such requirements before permitting them to access such records and information.

D. Use, Security, and Retention

Confidential Information of any kind shall not be distributed or sold to any third party or used by Contractor or its agents in any way, except as authorized by this Contract or approved in writing by the State. Contractor shall provide and maintain a secure environment that ensures confidentiality of all State records and other Confidential Information wherever located. Confidential Information shall not be retained in any files or otherwise by Contractor or its agents, except as permitted in this Contract or approved in writing by the State. All Confidential Information shall

be stored, processed, or transferred only in or to facilities located within the United States.

E. Disclosure-Liability

Disclosure of confidential State records or other Confidential Information by Contractor for any reason outside of the requirements of this Contract may be cause for legal action by third parties against Contractor, its Subcontractor(s), the State or their respective agents. Subject to Section 19.P, Contractor shall indemnify, save, and hold harmless the State, its employees and agents, against any and all third party claims, damages, liability and court awards, including costs, expenses, and attorney fees and related costs, incurred as a result of any act or omission by Contractor, or its employees, agents, Subcontractors, or assignees in violation of the terms and conditions of this **§10**, provided that the limitation set forth in Section 19.P shall not apply to any fines imposed by the Department of Health and Human Services for a violation of HIPAA, consistent with Section 7 of the Business Associate Addendum.

11. CONFLICTS OF INTEREST

A. Conflict of Interest

Contractor shall not engage in any business or personal activities or practices or maintain any relationships which conflict in any way with the full performance of Contractor's obligations hereunder. Contractor acknowledges that with respect to this Contract, even the appearance of a conflict of interest is harmful to the State's interests. Absent the State's prior written approval, Contractor shall refrain from any practices, activities or relationships that reasonably appear to be in conflict with the full performance of Contractor's obligations to the State hereunder. If a conflict or appearance exists, or if Contractor is uncertain whether a conflict or the appearance of a conflict of interest exists, Contractor shall submit to the State a disclosure statement setting forth the relevant details for the State's consideration. Failure to promptly submit a disclosure statement or to follow the State's direction in regard to the apparent conflict constitutes a breach of this Contract.

B. Written Code of Standards

Contractor (and Subcontractors permitted under the terms of this Contract) shall maintain a written code of standards governing the performance of its employees engaged in the award and administration of contracts. No employee, officer or agent of Contractor, or any Subcontractor shall participate in the selection, or in the award or administration of a contract or subcontract supported by federal funds if a conflict of interest, real or apparent, would be involved. Such a conflict would arise when:

i. The employee, officer or agent;
ii. Any member of the employee's immediate family;
iii. The employee's partner; or
iv. An organization which employs, or is about to employ, any of the above, has a financial or other interest in the firm selected for award. Contractor's or Subcontractors' officers, employees, or agents will neither solicit nor accept gratuities, favors, or anything of monetary value from Contractors, potential Contractors, or parties to subagreements.

12. REPRESENTATIONS AND WARRANTIES

Contractor makes the following specific representations and warranties, each of which was relied on by the State in entering into this Contract.

A. Standard and Manner of Performance

Contractor represents and warrants that it shall perform its obligations hereunder in a professional and workmanlike manner and in the sequence and manner set forth in this Contract.

B. Legal Authority – Contractor Signatory

Contractor represents and warrants that it possesses the legal authority to enter into this Contract and that it has taken all actions required by its procedures, and bylaws, and/or applicable laws to exercise that authority, and to lawfully authorize its undersigned signatory to execute this Contract, or any part thereof, and to bind Contractor to its terms. If requested by the State, Contractor shall provide the State with proof of Contractor's authority to enter into this Contract within fifteen (15) days of receiving such request.

C. Licenses, Permits, Etc.

Contractor represents and warrants that as of the Effective Date and at all times thereafter have and maintain, at its sole expense, all licenses, certifications, approvals, insurance, permits and other Authorizations required by law to perform its obligations hereunder. Contractor warrants that it shall maintain all necessary licenses, certifications, approvals, insurance, permits, and other Authorizations required to properly perform this Contract, without reimbursement by the State or other adjustment in Contract Funds. Additionally, all employees, agents, and Subcontractors of Contractor performing Services under this Contract shall hold all required licenses or certifications, if any, to perform their responsibilities. Contractor, if a foreign corporation or other foreign entity transacting business in the State of Colorado, further warrants that it currently has obtained and shall maintain any applicable certificate of authority to transact business in the State of Colorado and has designated a registered agent in Colorado to accept service of process. Any revocation, withdrawal or non-renewal of licenses, certifications, approvals, insurance, permits or any such similar requirements necessary for Contractor to properly perform the terms of this Contract is a material breach by Contractor and constitutes grounds for termination of this Contract.

D. Disabling Code

Contractor represents and warrants that it will use up-to-date commercial anti-virus software to detect and remove viruses and other malware from software before delivering it to the State. Contractor will not introduce into the PBMS or any State system any virus, worm, trap door, back door, timer, clock, counter, or other limiting routine, instruction, or design that would erase data or programming or otherwise cause the PBMS or any State system to become inoperable or incapable of being used in the full manner for which it was designed and created (collectively, "Disabling Code"). In the event a Disabling Code is introduced by Contractor, Contractor shall take all steps necessary, at no additional cost to the State, to remove or remedy the Disabling Code and to restore and/or reconstruct any and all data lost by the State as

a result of such Disabling Code. The foregoing shall not apply to any Disabling Code introduced by the State or its employees or agents. In the event that Disabling Code is introduced into the PBMS or a related State system in any manner other than by Contractor, if requested by the State, Contractor shall take all steps necessary, through the Change Management Process, to remove or remedy the Disabling Code and to restore and/or reconstruct any and all data lost by the State as a result of such Disabling Code.

E. Third Party Warranties and Indemnities

For any third party software provided by Contractor to the State, to the extent possible, Contractor hereby assigns to the State all end-user warranties and indemnities relating to such third party software. To the extent that it is not possible for Contractor to assign any of such end-user warranties and indemnities through to the State, Contractor shall take reasonable steps to enforce such warranties and indemnities on behalf of the State to the extent Contractor is permitted to do so under the terms of the applicable third party agreements.

F. Open Source Software

Other than as specified in the Contract, Contractor will provide ten (10) days' notice to the State before introducing into the PBMS any "open source," "free software," or "freeware" of any kind or any programming or software that is subject to licensing terms requiring any intellectual property owned or licensed by the State to be generally (i) disclosed or distributed in source code or object code form; (ii) licensed for the purpose of making derivative works; or (iii) redistributable. The Contractor shall not introduce into the PBMS any new "open source", "free software" or "freeware" described in this section without the prior, written consent of the Department.

13. INSURANCE

Contractor and its Subcontractors appropriate to the subcontractor's activities within this Contract, shall maintain insurance as specified in this section at all times during the term of this Contract. All policies evidencing the insurance coverage required hereunder shall be issued by insurance companies with an AM Best rating of not less than VII.

A. Contractor

i. Public Entities

If Contractor is a "public entity" within the meaning of the Colorado Governmental Immunity Act, CRS §24-10-101, *et seq*., as amended (the "GIA"), then Contractor shall maintain at all times during the term of this Contract such liability insurance, by commercial policy or self-insurance, as is necessary to meet its liabilities under the GIA. Contractor shall provide a certificate of insurance to the State, if requested by the State. Contractor shall require each contract with a Subcontractor that is a public entity, to maintain the insurance requirements necessary to meet such Subcontractor's liabilities under the GIA appropriate to the subcontractor's activities within this Contract.

ii. Non-Public Entities

If Contractor is not a "public entity" within the meaning of the GIA, Contractor shall maintain during the term of this Contract insurance coverage meeting the requirements set forth in **§13.B** and with respect to

Subcontractors that are not "public entities," Contractor shall require subcontractors to maintain the insurance requirements as outlined below, appropriate to the subcontractor's activities within this Contract.

B. Contractors – Subcontractors

Contractor shall require Subcontractors other than those that are public entities, providing Goods or Services in connection with this Contract, to maintain insurance requirements substantially similar to the following, appropriate to the subcontractors' activities within this Contract:

i. Worker's Compensation

Worker's Compensation Insurance as required by State statute, and Employer's Liability Insurance with a limit of $1,000,000 per accident covering all of Contractor's employees acting within the course and scope of their employment.

ii. General Liability

Commercial General Liability Insurance written on ISO occurrence form CG 00 01 or equivalent, covering premises operations, Damage to Premises Rented to You, independent contractors, products and completed operations, contractual liability, personal injury, and advertising liability with limits as follows:

a. $1,000,000 each occurrence;

iii. Reserved

iv. Automobile Liability

Automobile Liability Insurance covering any auto (including owned, hired and non-owned autos) with a limit of $1,000,000 each accident combined single limit.

v. Professional Liability Insurance

Professional Liability Insurance covering financial loss caused by an error, omission or any negligent acts, including loss of Protected Health Information data or claims based upon alleged violations of privacy rights through improper use or disclosure of Protected Health Information, with limits as follows:

a. $1,000,000 each claim; and
b. $1,000,000 general aggregate.

vi. Crime Insurance

Crime Insurance including Employee Dishonesty coverage with limits as follows:

a. $1,000,000 each occurrence; and
b. $1,000,000 general aggregate.

vii. Additional Insured

The State shall be included as additional insured on all Commercial General Liability and Automobile Liability Insurance policies required of Contractor and any Subcontractors hereunder.

viii. Primacy of Coverage

General Liability coverage required of Contractor and Subcontractor shall be primary over any insurance or self-insurance program carried by the State.

ix. Cancellation

The above insurance policies shall include provisions requiring notification of cancellation or non-renewal to Contractor and Contractor shall forward such notice to the State in accordance with §16 (Notices and Representatives) within seven (7) days of Contractor's receipt of such notice.

x. Subrogation Waiver

To the extent available, the workers' compensation insurance policy, the general liability insurance policy and the auto insurance policy maintained by Contractor or its Subcontractors shall include a clause stating that it shall waive all rights of recovery, under subrogation or otherwise, against Contractor or the State, its agencies, institutions, organizations, officers, agents, employees, and volunteers.

C. Certificates

Contractor and all Subcontractors shall provide certificates of all insurance showing insurance coverage required hereunder to the State within seven (7) Business Days of the Effective Date of this Contract. No later than ten (10) calendar days after renewal of any such coverage, Contractor and each Subcontractor shall deliver to the State or Contractor certificates of insurance evidencing renewals thereof. In addition, upon request by the State at any other time during the term of this Contract or any subcontract, Contractor and each Subcontractor shall, within fifteen (15) days of such request supply to the State a certificate of insurance evidencing compliance with the provisions of this **§13**.

14. BREACH

A. Defined

In addition to any breaches specified in other sections of this Contract, the failure of Contractor to perform any of its material obligations hereunder in whole or in part consistent with the requirements set forth in this Contract constitutes a breach. Contractor shall have the right to dispute any such breach in accordance with the Dispute Process in **§20.E**. The institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within twenty (20) days after the institution or occurrence thereof, shall also constitute a breach.

B. Notice and Cure Period

In the event of a breach, the State shall notify Contractor of such in writing in the manner provided in **§16**. If such breach is not cured within thirty (30) calendar days of receipt of written notice or an alternative cure period agreed upon by the Parties prior to the end of such 30 calendar day period, the State may exercise any of the remedies set forth in **§15**. Notwithstanding anything to the contrary herein, the State, in its sole discretion, need not provide advance notice or a cure period and may immediately terminate this Contract in whole or in part if reasonably necessary to preserve public safety or to prevent immediate public crisis, or take such other action as may be necessary to prevent irreparable harm. Contractor shall have the right to dispute any breach notification in accordance with the Dispute Process in **§20.E**.

15. REMEDIES

A. Termination for Cause and/or Breach

If Contractor is in breach under any provision of this Contract, the State shall have all of the remedies listed in this **§15** in addition to all other remedies set forth in other sections of this Contract, and without limiting its remedies otherwise available at law or equity, following the notice and cure period set forth in **§14.B**. The State may exercise any or all of the remedies available to it, in its sole discretion, concurrently or consecutively. The State may terminate this entire Contract or any part of this Contract. Exercise by the State of this right shall not be a breach of its obligations hereunder.

i. Obligations and Rights

To the extent specified in any termination notice, Contractor shall not incur further obligations or render further performance hereunder past the effective date of such notice, and shall terminate outstanding orders and subcontracts with third parties, except as provided below. However, Contractor shall complete and deliver to the State all Work, Work Product, Services and Goods not previously delivered and not cancelled by the termination notice and may incur obligations as are necessary to do so within this Contract's terms. Such Work, Work Product, Services and Goods shall be the property of the State. The State shall obtain good and clear title to all such Work, Work Product, Services and Goods upon delivery, and Contractor shall provide reasonable assistance to the State to establish, confirm, evidence or enforce such good and clear title. Contractor shall provide a list of all licenses which it currently owns that are used in connection with the PBMS, including all licenses described in the License Table in Exhibit E, Section 1.1.1.3.1, and shall either a) transfer such licenses to the State at no cost to the State, b) provide the State with the right to use the underlying software, if the State enters into a mutually acceptable agreement with the Contractor for the continued use of the software or c) if the Contractor is unable to transfer the licenses and cannot provide the State with the right to use the software, it shall be liable for the cost required to be paid by the State to acquire equivalent licenses. Contractor shall continue performance of this Contract up to the effective date of the termination notice. To the extent the Contract is not terminated, if any, Contractor shall continue performance until the expiration of this Contract. At the sole discretion of the State, Contractor shall assign to the State if possible or reasonably assist the State in the assignment to the State of all right, title, and interest under such terminated orders or subcontracts. Upon termination, Contractor shall take timely, reasonable and necessary action to protect and preserve property in the possession of Contractor in which the State has an interest. All materials owned by the State and all Confidential Information of the State in the possession of Contractor shall be promptly returned to the State or destroyed by Contractor if approved by the State unless otherwise required by law. Contractor shall be obligated to return any payment advanced under the provisions of this Contract. Any advanced payments will be specifically identified in the Contract.

ii. Payments

Upon termination, and subject to the withholding provisions of this Contract, the State shall reimburse Contractor for work performed and accepted in

conformance with the requirements specified in this Contract up to the effective date of the termination. If, after termination by the State, it is determined that Contractor was not in breach or that Contractor's action or inaction was excusable, such termination shall be treated as a termination in the public interest and the rights and obligations of the Parties shall be the same as if this Contract had been terminated in the public interest, as described herein.

iii. Damages and Withholding

Notwithstanding any other remedial action by the State, Contractor shall remain liable to the State for any damages sustained by the State by virtue of any breach under this Contract by Contractor and the State may withhold any payment to Contractor, after written notice, as reasonably necessary for the purpose of mitigating the State's damages, until such time as the exact amount of damages due to the State from Contractor is determined or the breach is cured and all damages to the State have been fully mitigated. If the Contract is terminated for default, the State may withhold any amount that may be due Contractor as the State deems reasonably necessary to protect the State against loss, including loss as a result of outstanding liens, claims of former lien holders, or for the reasonable excess costs incurred in procuring similar goods or services related to the termination for default. Contractor shall be liable for reasonable excess costs incurred by the State in procuring from third parties replacement Work, Services or substitute Goods as cover for such termination for default.

iv. Right to Set Off.

The State shall have the right to set off any amounts owed to Contractor against any damages or charges assessed by the State against Contractor.

v. Abandonment

a. Contractor shall not "Abandon" the Work. For the purposes of this Contract, "Abandon," or "Abandonment" means: Contractor's actual willful non-performance of any material aspects of the Work in breach of the Contract, and which results in a material adverse effect on (i) the ability of the State to timely and properly receive and/or use the PBMS, or (ii) critical aspects of the State's internal operations or financial reporting requirements. In the event of an Abandonment, in addition to the other remedies it may have, the State may seek specific performance in a court of competent jurisdiction without the need to demonstrate irreparable harm. The State shall not implement this remedy if the Dispute Process has been completed by both parties and the State fails to make undisputed payments in a timely manner in violation of the terms of this Contract.

b. In the event of an Abandonment, in addition to the other remedies it may have, State may, but shall not be required to (a) terminate this Contract for cause upon notice to Contractor pursuant to Section **§14**; or (b) seek specific performance of the Contract. In addition, in the event of an Abandonment, upon request by the State, Contractor shall provide, at no additional cost to State, all services and meet all requirements for the Turnover Phase, as described in **Exhibit D**, Project Phase Document, and all services and requirements contained

within **Exhibit C**, Requirements, that are related to the Turnover Phase and Turnover Plan, which will last no more than twelve (12) months. These requirements include all requirements of **Exhibit C**, Requirements, Section 15, COMMIT Project Phases, Turnover Phase. The exercise of State's rights under this section shall not waive or release any rights, claims or remedies that State may have for the Abandonment. The Contractor and the State shall mitigate any damages that accrue as a result of Abandonment. Notwithstanding anything contained herein to the contrary, Contractor expressly waives and disclaims any right or remedy it may have to discontinue the performance of the Work or any portion thereof.

B. Early Termination in the Public Interest

The State is entering into this Contract for the purpose of carrying out the public policy of the State of Colorado, as determined by its Governor, General Assembly, and/or courts. If this Contract ceases to further the public policy of the State, the State, in its sole discretion, may terminate this Contract, in whole or in part. Exercise by the State of this right shall not constitute a breach of the State's obligations hereunder. This subsection shall not apply to a termination of this Contract by the State for cause or breach by Contractor, which shall be governed by **§15.A** or as otherwise specifically provided for herein.

i. Method and Content

The State shall notify Contractor of such termination in accordance with **§16.** The notice shall specify the effective date of the termination, and whether it affects all or a portion of this Contract. The State shall provide Contractor with as much notice as is reasonably possible under the circumstances.

ii. Obligations and Rights

Upon receipt of a termination notice, Contractor shall be subject to and comply with the same obligations and rights set forth in **§15.A.i**.

iii. Payments

If this Contract is terminated by the State pursuant to this **§15.B**, Contractor shall be paid for work performed and accepted in accordance with the requirements of this Contract. Additionally, if this Contract is less than 60% completed upon the effective date of such termination, the State may reimburse Contractor for actual out-of-pocket expenses (not otherwise reimbursed under this Contract) incurred by Contractor prior to the effective date of the termination in the public interest which are directly attributable to the uncompleted portion of Contractor's obligations hereunder; provided that the sum of any and all reimbursement shall not exceed the maximum amount payable to Contractor hereunder.

C. Additional Remedies

The State, in its sole discretion, may exercise one or more of the following remedies in addition to other remedies available to it:

i. Suspend Performance

Suspend Contractor's performance with respect to all or any portion of this Contract, pending necessary corrective action as specified by the State without entitling Contractor to an adjustment in price/cost or performance

schedule, based on Contractor's failure to perform the suspended portions of the Contract in accordance with the Contract's requirements. Contractor shall promptly cease performance and shall promptly cease incurring costs in accordance with the State's directive and the State shall not be liable for costs incurred by Contractor after the suspension of performance under this provision.

ii. Withhold Payment

Withhold payment to Contractor until Contractor's performance or corrections in Contractor's performance are satisfactorily made and completed in accordance with this Contract as reasonably necessary for the purpose of mitigating the State's damages, until such time as the exact amount of damages due to the State from Contractor is determined or the breach is cured and all damages to the State have been fully mitigated.

iii. Deny Payment

Deny payment for those obligations not performed or that cannot be performed, to the extent due to Contractor's actions or inactions; provided, that any denial of payment shall be associated with only the obligations not performed in accordance with this Contract.

iv. Removal

The State may request removal from work on the Contract of any of Contractor's employees, agents, or Subcontractors whom the State reasonably determines to be incompetent, careless, insubordinate, unsuitable, or otherwise unacceptable, or whose continued relation to this Contract is deemed to be contrary to the public interest or the State's best interest. For any requested removal of Contractor's employees, agents or Subcontractors, in a non-emergency situation, the State shall provide written notice to Contractor identifying each element of dissatisfaction and Contractor shall have ten (10) Business Days from receipt of such written notice to provide the State with a written action plan to remedy each stated point of dissatisfaction. In the event of an emergency, the representatives described in section 16 will meet within 24 hours to determine an expeditious resolution. In the event that completion of the action plan fails to reasonably remedy all stated points of dissatisfaction, Contractor shall remove the employees, agents or Subcontractors as requested by the State**.**

v. Equitable Relief

The State may seek immediate equitable remedies if believed necessary to prevent irreparable harm, and the State is not required to provide notice and opportunity to cure in such situations.

D. Multiple Remedies.

The State may exercise multiple remedies as provided in this Contract or by applicable law, provided that the State shall not receive double recovery for actual damages.

E. Liquidated Damages

i. Contractor acknowledges that late or improper completion of the PBMS will cause loss and damage to the State, and that it would be impracticable and extremely difficult to determine the actual damage sustained by the State as a result; it is for this reason that the Parties have agreed, pursuant to this Section § **15.E**, that liquidated damages will be imposed if certain delays in Quarterly

Milestones are experienced. The Parties agree that the amount of liquidated damages specified in this **§15.E** represents a reasonable estimation of damages that will be suffered by the State for late or improper performance. Liquidated damages may be deducted by the State from any money payable to Contractor pursuant to this Contract related to Contractor's failure to meet Quarterly Milestones as set forth below:

a. If a Quarterly Milestone is missed, then Contractor must analyze whether any changes are necessary to the mutually agreed timeline and provide an updated timeline to the State for approval by the State.

b. The date when a Quarterly Milestone is due from Contractor and the Operational Start Date in effect at the time when the Quarterly Milestone is due are set forth in the Project Management Plan, as described in **Exhibit C**, Requirements.

ii. If Contractor's failure to meet a Quarterly Milestone increases the Operational Start Date in effect at the time when the Quarterly Milestone is due, the State may assess damages in the amount of $4,000 per Business Day until the Quarterly Milestone is met.

iii. If Contractor's failure to meet a Quarterly Milestone does not increase the Operational Start Date, the State may assess damages in the amount of $1,000 per Business Day until the Quarterly Milestone is met.

iv. The deliverable and acceptance for a Quarterly Milestone shall be that as established in **Exhibit A**, Statement of Work, Section 5.

a. If Contractor does not deliver a Quarterly Milestone by the date established in the Project Management Plan then damages will be assessed starting on the date that the Quarterly Milestone was due.

b. If the Department directs Contractor to make changes to the Quarterly Milestone deliverable or if the entire Quarterly Milestone deliverable is rejected, and if Contractor makes changes such that Quarterly Milestone deliverable is accepted by the State the within the timeframe as specified in **Exhibit A**, Statement of Work, Section 5 then no damages will be assessed.

c. If the Department directs Contractor to make changes to the Quarterly Milestone deliverable or if the entire Quarterly Milestone deliverable is rejected, and if Contractor does not make changes such that Quarterly Milestone deliverable is accepted by the State the within the timeframe as specified in **Exhibit A**, Statement of Work, Section 5 then damages will be assessed starting on the date that Contractor's timeframe has ended as specified in **Exhibit A**, Statement of Work, Section 5.

d. Damages will not be assessed during the timeframe that a Quarterly Milestone is being reviewed by the State.

v. Contractor may dispute liquidated damages in accordance with §**20.E** if Contractor believes it is not at fault or if the liquidated damages are not assessed correctly (e.g., per Business Day amount, the number of Business Days assessed under the liquidated damages) or that damages are the result of acts or omissions of the State or its agents or events of Force Majeure.

vi. For any liquidated damages assessed under Section **15.E.ii**:

a. If the Parties subsequently agree, or it is determined by the outcome of the Dispute Process, that the failure to meet the Quarterly Milestone will not delay the Operational Start Date in effect at the time when the Quarterly Milestone was due, any liquidated damages assessed for such failure will be reduced to $1,000 per Business Day; and

b. If Contractor meets the Operational Start Date in effect at the time when the Quarterly Milestone was due, any liquidated damages that were previously assessed under Section **15.E.ii** and not reduced pursuant to **Section 15.E.v.a.** above will be reduced to $1,000 per Business Day.

For Example:

If the Quarterly Milestone is due on March 31st (assuming March 31st is a Monday), is delivered on April 11th then there are 10 days of damages.

If the Quarterly Milestone is due on March 31st, is delivered on March 31st, the State reviews for 10 days, and accepts, then no damages.

If the Quarterly Milestone is due on March 31st, is delivered on March 31st, the State reviews for 10 days, and requests changes or rejects, Contractor has 10 days to fix with no damages.

If the Quarterly Milestone is due on March 31st, is delivered on March 31st, the State reviews for 10 days, and requests changes or rejects, if Contractor does not return a revised Quarterly Milestone, the damages start immediately after Contractor's 10 days ends. If Contractor returns the revised Quarterly Milestone on day 12, then only two days of damages would be assessed.

If the Quarterly Milestone is due on March 31st, is delivered on March 31st, the State reviews for 10 days and requests changes or rejects, Contractor has 10 days to fix with no damages. Then, the State has five days to review and request changes again, and then Contractor has another five days to fix again, then there begins a two day turn around for the State and Contractor to review and fix. This can continue without any damages assuming that everyone meets their timeline and the Quarterly Milestone is eventually fixed.

F. Other damages

i. Following November 1, 2017, damages shall be imposed if claims processing is not fully operational and the PBMS is not operational as described in **Exhibit C**, Requirements, and Contractor is determined to be at fault for the delay based on the outcome resulting from the Dispute Process (as described in **§20.E**). Damages will be assessed on a monthly basis based on the increase in the incremental difference between the amount that must be paid to the current MMIS contractor and the contractual amount to be paid to Contractor. Contractor and the State will in good faith mitigate, to the extent possible, any damages. Contractor will not be paid any amount during such delay. This Section 15.F.i. may only be modified through a formal Contract amendment under Section 19.H.i and the date may not be extended through the use of the Project Management Plan.

ii. If CMS certification is not granted within eighteen (18) months of the first day of the PBMS Ongoing Operations and Enhancements Contract Stage, and Contractor is determined to be at fault for the delay based on the outcome resulting from the Dispute Process (as described in Section

§20.E) Contractor will reimburse the Department an amount equal to the difference between the 75% Federal Financial Participation rate for a CMS certified system and the 50% Federal Financial Participation rate the Department incurred for operating an non-CMS certified system during the period the system is not certified by CMS. If CMS certifies the MMIS back to Operational Start Date, then the State will equitably reimburse Contractor for the amounts that were assessed under this Section (ii).

G. Damages Disputes

All damages will be assessed via the Dispute Process (as described in **§20.E**) for any BIDM or MMIS implementation delays or unmet contractual obligations that impact the PBMS implementation.

H. Warranty Period

The first 365 calendar days beginning on the first day of the PBMS Ongoing Operations and Enhancements Contract Stage shall be considered the "Warranty Period". The Warranty Period covers the agreed upon functionality and Contractor shall be responsible to correct all Defects in order to allow the PBMS to operate according to Contract requirements and Specifications. Contractor does not necessarily need to correct all Defects during the Warranty Period, but all Defects identified by the Department or Contractor during the Warranty Period shall be corrected by Contractor within a reasonable timeframe at its expense and at no additional cost to the Department, or as agreed upon through the Change Management Process. Contractor will maintain routine PBMS performance while correcting the Defects.

16. NOTICES AND REPRESENTATIVES

Each individual identified below is the principal representative of the designating Party. Unless otherwise required by a specific provision of this Contract, all notices required to be given hereunder shall be hand delivered with receipt required or sent by certified or registered mail to such Party's principal representative at the address set forth below. In addition to, but not in lieu of, a hard-copy notice, notice also may be sent by e-mail to the e-mail addresses, if any, set forth below. Either Party may from time to time designate by written notice substitute addresses or persons to whom such notices shall be sent. Unless otherwise provided herein, all notices shall be effective upon receipt.

For the State:
Parrish Steinbrecher, Provider Payment Division Director
Department of Health Care Policy and Financing
1570 Grant Street
Denver, Colorado 80203
Parrish.Steinbrecher@state.co.us

For Contractor:
Teresa Elam, Senior Director, Account Management
Magellan Medicaid Administration, Inc.
11013 West Broad Street, Suite 500
Glen Allen, VA 23060
RACoppola@magellanhealth.com

17. RIGHTS IN DATA, DOCUMENTS, AND COMPUTER SOFTWARE

A. Ownership.

All software, information and materials and all intellectual property rights in and to such software, information and materials owned by Contractor prior to the Effective Date (collectively "Contractor Property") shall be the sole and exclusive property of Contractor. All Work, Work Product and Goods shall be the property of the State. The State shall obtain good and clear title to all such Work, Work Product and Goods and Contractor shall provide reasonable assistance to the State to establish, confirm, evidence or enforce such good and clear title. All Work, Work Product, Goods and all intellectual property rights in and to such Work, Work Product, and Goods developed or invented pursuant to this Contract, or otherwise resulting from this Contract, (collectively "State Property") shall be the sole and exclusive property of the State. The PBMS will be licensed in accordance with 42 CFR § 495.360, 45 CFR § 95.617, and 45 CFR § 92.34, software and ownership rights. To the extent that any State Property may be considered a "work made for hire" within the meaning of the Copyright Act of 1976, as amended (the "Copyright Act"), the parties agree that such State Property shall be considered a work made for hire. If and to the extent that any State Property may not be considered a "work made for hire" within the meaning of the Copyright Act, Contactor agrees that all exclusive right, title and interest in and to such State Property, and all copies thereof, are hereby expressly assigned automatically to the State without further consideration. Any agreement entered into by Contractor and a third party which may or does relate to the creation, development, invention of any State Property shall include terms that ensure that the State obtains the same rights in the State Property generated under such agreement as those set forth in this **§17.A**. Contractor agrees to reasonably assist the State in confirming, obtaining and enforcing all rights and other legal protections for the State Property and to execute any and all documents that the State may reasonably request in connection therewith, including without limitation any patent or copyright assignment document(s), without additional cost to the State. To the extent that any State Property constitutes a derivative work as defined in the Copyright Act, upon request by the State, Contractor shall identify the nature of the preexisting work(s), their owner and the source of Contractor's authority to create the derivative work.

B. Licenses.

Contractor hereby grants to the State a perpetual, irrevocable, non-exclusive, royalty free license, with the right to sublicense to Third Party Users, to make, use, reproduce, distribute, perform, display, create derivatives of and otherwise exploit all Contractor Property provided pursuant to this Contract that is incorporated in or necessary for the use, development, installation, Maintenance and revision of the PBMS, except for Contractor Property identified in **Exhibit E**, Compensation and Quality Maintenance Payments, Section 1.1.1.3.2. The State hereby grants to Contractor a perpetual, non-exclusive, royalty free license to reproduce, publish, use, copy and modify the deliverables under this Contract for the purpose of providing services to its other customers that are similar to the services under this Contract. PBMS Source Code will be made available to the State upon request with thirty (30) days previous notice and be made available quarterly to the State.

C. Third Party Property.

For any property or intellectual property rights of third parties, including without limitation software, used in or incorporated in the PBMS by Contractor, or necessary for the use of the PBMS by the State, (collectively "Third Party Property") Contractor

shall obtain and maintain, without additional cost to the State, all necessary rights for Contractor and the State to use all Third Party Property for the purposes contemplated by this Contract. For all Third Party Property that comprises software, Contractor will provide copies of all licenses applicable to such software to the State upon reasonable request by the State and at the time of the Turnover Phase, as defined in **Exhibit D**, Project Phase Document.

D. Underlying Technology.
Nothing contained in this Contract will restrict either party from using any ideas, concepts, know how, methodologies processes, technologies, algorithms, or techniques that either party, individually or jointly, develops or discloses under this Contract, provided that in doing so the party does not breach its confidentiality obligations or infringe the intellectual property rights of the other party or third parties who have licensed or provided materials to the other party. Nothing in this Contract will prevent either party from independently developing any software or technology that is the same or similar to any software or technology owned by the other party so long as the developing party does not infringe or misappropriate any intellectual property rights of the other party.

E. Avoidance of Infringement.
In performing under this Contract, Contractor agrees to avoid designing or developing any items that infringe one or more patents or other intellectual property rights of any third party. If Contractor becomes aware of any such possible infringement during in the course of performing under this Contract, Contractor shall immediately inform the State in writing.

F. Indemnification.
Contractor will defend, indemnify and hold the State harmless from and against any and all claims, actions, losses, liability, damages, costs, and expenses (including attorney's fees, expert witness fees, and court costs) directly or indirectly arising from or related to any actual or alleged infringement (including contributory infringement), misappropriation, or violation of any third party's patents, copyrights, trade secret rights, trademarks, or other intellectual property or proprietary rights of any nature in any jurisdiction in the world, relating to any Contractor Property or State Property or any portion thereof, or the use thereof by the State or its agents or employees. The State shall: (i) give Contractor written notice within thirty (30) days of receipt by the State of notice of such claim or action; and (ii) allow Contractor to control, and provide reasonable assistance and cooperation to the Contractor in connection with such claim or action and all related negotiations. Contractor shall keep the State advised of any defense or settlement. Contractor shall not enter into any stipulated judgment or settlement that purports to bind the State without the State's express written Authorization, which shall not be unreasonably withheld or delayed. The State may, at its discretion, participate in any defense. The foregoing obligations shall not apply to the extent such infringement results from or is based on (i) any use of the product or service or modifications to the product or service by the State that was not contemplated by Contractor, described in this Contract, or related to the PBMS, or (ii) the combination by the State of such product or service with any equipment, software or other materials that were not provided or expressly approved by Contractor. For

the avoidance of doubt, the obligations of Contractor under this Section **17.F** are not subject to Section **19.P**.

G. If any Contractor Property or State Property or any portion thereof, or the use thereof by the State or its agents or employees, is found to infringe (including contributory infringement), misappropriate, or violate a third party's patent, copyright, trade secret right, trademark, or other intellectual property or proprietary rights of any nature in any jurisdiction in the world, and the completion, implementation or use pursuant to this Contract of any such Contractor Property or State Property or any portion thereof is impaired thereby, Contractor shall, at no charge to the State, and in addition to the State's other rights and remedies, (a) secure for the State and Contractor, to the extent necessary, the right to complete, implement, and use such Contractor Property or State Property as allowed under this Contract, (b) if (a) is not reasonably available, modify or replace Contractor Property or State Property so that they are non-infringing and provide similar features, functionality, or performance, or (c) if (b) is not reasonably available, refund to the State all amounts paid for Contractor Property or State Property under this Contract.

H. The obligations described in this section **§17** shall survive the termination, expiration, cancellation or non-renewal of this Contract. Contractor shall be liable for all costs and expenses incurred by the State under this **§17** and shall reimburse and indemnify the State such costs and expenses. Except for Contractor's liability under §§17.F, which shall be unlimited, Contractor's liability under this §17 shall be subject to the limitations of §19.P.

18. GOVERNMENTAL IMMUNITY

Liability for claims for injuries to persons or property arising from the negligence of the State of Colorado, its departments, institutions, agencies, boards, officials, and employees is controlled and limited by the provisions of the Colorado Governmental Immunity Act, CRS §24-10-101, *et seq.*, and the risk management statutes, CRS §24-30-1501, *et seq.*, as now or hereafter amended or as otherwise provided by law.

19. GENERAL PROVISIONS

A. Assignment and Subcontracts

Contractor's rights and obligations hereunder are personal and may not be transferred, assigned or subcontracted without the prior, written consent of the State. Any attempt at assignment, transfer or subcontracting without such consent shall be void. All assignments, subcontracts, or Subcontractors approved by Contractor and the State are subject to all of the provisions hereof. Contractor shall be solely responsible for all of the Work performed under this Contract, regardless of whether Subcontractors are used and for all aspects of subcontracting arrangements and performance. Copies of any and all subcontracts entered into by Contractor to perform its obligations hereunder shall be in writing and submitted to the State upon request. Any and all subcontracts entered into by Contractor related to its performance hereunder shall require the Subcontractor to perform in accordance with the terms and conditions of this Contract and to comply with all applicable federal and state laws. Any and all subcontracts shall include a provision that such subcontracts are governed by the laws of the State of Colorado.

B. Binding Effect

Except as otherwise provided in **§19.A**, all provisions herein contained, including the benefits and burdens, shall extend to and be binding upon the Parties' respective heirs, legal representatives, successors, and assigns.

C. Captions

The captions and headings in this Contract are for convenience of reference only, and shall not be used to interpret, define, or limit its provisions.

D. Counterparts

This Contract may be executed in multiple identical original counterparts, all of which shall constitute one agreement.

E. Entire Understanding

This Contract represents the complete integration of all understandings between the Parties regarding the subject matter of this Contract and all prior representations and understandings, oral or written, related thereto are merged herein. Prior or contemporaneous additions, deletions, or other changes hereto shall not have any force or effect whatsoever, unless embodied herein.

F. Indemnification

Subject to Section **19.P**, Contractor shall indemnify, save, and hold harmless the State, its employees and agents, against any and all third party claims, actions, damages, liability and court awards, including costs, expenses, and reasonable attorney fees and related costs, incurred as a result of any act or omission by Contractor, or its employees, agents, Subcontractors, or assignees pursuant to the terms of this Contract; however, the provisions hereof shall not be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions, of the Colorado Governmental Immunity Act, CRS §24-10-101 *et seq.*, or the Federal Tort Claims Act, 28 U.S.C. 2671 *et seq.*, as applicable, as now or hereafter amended.

G. Jurisdiction and Venue

All suits or actions related to this Contract shall be filed and proceedings held in the State of Colorado and exclusive venue shall be in the City and County of Denver.

H. Modification

i. By the Parties

Except as specifically provided in this Contract, modifications of this Contract shall not be effective unless agreed to in writing by the Parties in an amendment to this Contract, properly executed and approved in accordance with applicable Colorado State law and State Fiscal Rules. Modifications permitted under this Contract, other than contract amendments, shall conform to the policies of the Office of the State Controller, including, but not limited to, the policy entitled MODIFICATIONS OF CONTRACTS - TOOLS AND FORMS.

ii. By Operation of Law

This Contract is subject to such modifications as may be required by changes in Federal or Colorado State law, or their implementing regulations. Any such required modification shall be reviewed through the Change Management Process to determine whether changes are required in the Contract.

I. Order of Precedence

The provisions of this Contract shall govern the relationship of the State and Contractor. In the event of conflicts or inconsistencies between this Contract and its exhibits and attachments, including, but not limited to, those provided by Contractor, such conflicts or inconsistencies shall be resolved by reference to the documents in the following order of priority:

i. Colorado Special Provisions
ii. HIPAA Business Associate Addendum and Attachment A
iii. The provisions of the main body of this Contract
iv. **Exhibit A**, Statement of Work
v. **Exhibit C**, Requirements
vi. **Exhibit G**, Performance Standards
vii. **Exhibit E**, Compensation and Quality Maintenance Payments
viii. **Exhibit D**, Project Phase Document
ix. **Exhibit F**, Terminology
x. **Exhibit B**, Sample Option Letter
xi. **Exhibit H**, State Cybersecurity Policies

The provisions of the main body of this Contract are not intended to supersede or limit the obligations and requirements set forth in the Exhibits.

J. Severability

Provided this Contract can be executed and performance of the obligations of the Parties accomplished within its intent, the provisions hereof are severable and any provision that is declared invalid or becomes inoperable for any reason shall not affect the validity of any other provision hereof, provided the Parties can continue to perform their obligations under this Contract in accordance with its intent.

K. Survival of Certain Contract Terms

Notwithstanding anything herein to the contrary, Sections **9, 10, 15, 17, 19, 20.E** and all provisions of this Contract requiring continued performance, compliance, or effect after termination, cancellation or expiration hereof, shall survive such termination, cancellation or expiration and shall be enforceable by the State if Contractor fails to perform or comply as required.

L. Taxes

The State is exempt from all federal excise taxes under IRC Chapter 32 (No. 84-730123K) and from all State and local government sales and use taxes under CRS §§39-26-101 and 201, *et seq*. Such exemptions apply when materials are purchased or services are rendered to benefit the State; provided, however, that certain political subdivisions (e.g., City of Denver) may require payment of sales or use taxes even though the product or service is provided to the State. Contractor shall be solely liable for paying such taxes as the State is prohibited from paying or reimbursing Contractor for such taxes.

M. Third Party Beneficiaries

Enforcement of this Contract and all rights and obligations hereunder are reserved solely to the Parties. Any services or benefits which third parties receive as a

result of this Contract are incidental to the Contract, and do not create any rights for such third parties.

N. Waiver

Waiver of any breach under a term, provision, or requirement of this Contract, or any right or remedy hereunder, whether explicitly or by lack of enforcement, shall not be construed or deemed as a waiver of any subsequent breach of such term, provision or requirement, or of any other term, provision, or requirement.

O. CORA Disclosure

To the extent not prohibited by federal law, this Contract and the performance measures and standards under CRS §24-103.5-101, if any, are subject to public release through the Colorado Open Records Act, CRS §24-72-101, *et seq*.

P. Limitation of Liability for PBMS Contract

The aggregate liability of Contractor, for this Contract only, under the agreement for claims other than indemnification for intellectual property infringement (**§17.F**), fines imposed by U.S. DHHS for violations of HIPAA (**§10.E**), bodily injury (including death) and damage to tangible personal property (including Software And Data) shall be limited to the following:

i. During the PBMS Implementation Contract Stage, as defined in **Exhibit A**, Statement of Work, twice the value of the original Contract for the PBMS Implementation Contract Stage, excluding any amounts added by amendment. In no event, shall Contractor be responsible for any indirect, punitive or consequential damages.

ii. During the PBMS Ongoing Operations and Enhancements Contract Stage, as defined in **Exhibit A**, Statement of Work, one times the value of the original Contract, for PBMS Ongoing Operations and Enhancements Contract Stage, excluding any amounts added by amendment. In no event shall Contractor be responsible for any indirect, punitive or consequential damages.

Q. No Construction Against Drafter

The Parties acknowledge that the terms of this Contract have been negotiated by the parties and agree that any principle of construction or rule of law that provides that an agreement shall be construed against the drafter of the agreement in the event of any inconsistency or ambiguity in such agreement shall not apply to the terms and conditions of this Contract.

20. ADDITIONAL GENERAL PROVISIONS

A. Compliance with Applicable Law

Contractor shall at all times during the Contract term strictly adhere to, and comply with, all applicable federal and state laws, and their implementing regulations. Contractor shall also require compliance with these statutes and regulations in subcontracts and subgrants permitted under this Contract. The federal laws and regulations include:

Age Discrimination Act of 1975, as amended	42 U.S.C. 6101, *et seq*.
Age Discrimination in Employment Act of 1967	29 U.S.C. 621-634

Americans With Disabilities Act of 1990 (ADA)	42 U.S.C. 12101, *et seq*.
Clean Air Act	42 U.S.C. 7401, *et seq*.
Equal Employment Opportunity	E.O. 11246, as amended by E.O. 11375, amending E.O. 11246 and as supplemented by 41 C.F.R. Part 60
Equal Pay Act of 1963	29 U.S.C. 206(d)
Federal Water Pollution Control Act, as amended	33 U.S.C. 1251, *et seq*.
Immigration Reform and Control Act of 1986	8 U.S.C. 1324b
Section 504 of the Rehabilitation Act of 1973, as amended	29 U.S.C. 794
Title VI of the Civil Rights Act of 1964, as amended	42 U.S.C. 2000d, *et seq*.
Title VII of the Civil Rights Act of 1964	42 U.S.C. 2000e
Title IX of the Education Amendments of 1972, as amended	20 U.S.C. 1681

State laws include:

Civil Rights Division	Section 24-34-301, CRS, *et seq*.

Contractor also shall comply with any and all laws and regulations prohibiting discrimination. In consideration of and for the purpose of obtaining any and all federal and/or state financial assistance, Contractor makes the following assurances, upon which the State relies.

i. Contractor will not discriminate against any person on the basis of race, color, national origin, age, sex, religion or handicap, including Acquired Immune Deficiency Syndrome (AIDS) or AIDS-related conditions, in performance of Work under this Contract.

ii. At all times during the performance of this Contract, no qualified individual with a disability shall, by reason of such disability, be excluded from participation in, or denied benefits of the service, programs, or activities performed by Contractor, or be subjected to any discrimination by Contractor.

Contractor shall take all necessary affirmative steps, as required by 45 C.F.R. 92.36(e), Colorado Executive Order and Procurement Rules, to assure that small and minority businesses and women's business enterprises are used, when possible, as sources of supplies, equipment, construction, and services purchased under this Contract.

B. Federal Audit Provisions

Office of Management and Budget (OMB) Circular No. A-133, Audits of States, Local Governments, and Non-Profit Organizations, defines audit requirements under the Single Audit Act of 1996 (Public Law 104-156). All state and local governments and non-profit organizations expending $500,000.00 or more from all sources (direct or from pass-through entities) are required to comply with the provisions of Circular No. A-133. The Circular also requires pass-through entities to monitor the activities of subrecipients and ensure that subrecipients meet the audit requirements. To identify its pass-through responsibilities, the State of Colorado requires all subrecipients to notify the State when expected or actual expenditures of federal assistance from all sources equal or exceed $500,000.00.

C. Debarment and Suspension

i. If this is a covered transaction or the Contract amount exceeds $100,000.00, Contractor certifies to the best of its knowledge and belief that it and its principals and Subcontractors are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any federal department or agency.

ii. This certification is a material representation of fact upon which reliance was placed when the State determined to enter into this transaction. If it is later determined that Contractor knowingly rendered an erroneous certification, in addition to other remedies available at law or by contract, the State may terminate this Contract for default.

iii. Contractor shall provide immediate written notice to the State if it has been debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded by any federal department or agency.

iv. The terms “covered transaction,” “debarment,” “suspension,” “ineligible,” “lower tier covered transaction,” “principal,” and “voluntarily excluded,” as used in this paragraph, have the meanings set out in 2 C.F.R. Parts 180 and 376.

v. Contractor agrees that it will include this certification in all lower tier covered transactions and subcontracts that exceed $100,000.00.

D. Force Majeure

Neither Contractor nor the State shall be liable to the other for any delay in, or failure of performance of, any covenant or promise contained in this Contract, nor shall any delay or failure constitute default or give rise to any liability for damages if, and only to the extent that, such delay or failure is caused by "Force Majeure." As used in this Contract, “Force Majeure” means acts of God; acts of the public enemy; acts of the state or any governmental entity in its sovereign or contractual capacity; fires; floods; epidemics; quarantine restrictions; strikes or other labor disputes; freight embargoes; unusually severe weather or other acts or events outside the reasonable control of a Party.

E. Dispute Process

i. Contractor and the State will follow the Dispute Process as outlined in this **§20.E**. The Dispute Process will be used for all disputes or disagreements (“Dispute”) between the State and Contractor.

a. A Type 1 Dispute is one that is considered severe enough to negatively impact the timeline for development or implementation of

the PBMS or the continued operation of the PBMS or Services, or that has a direct financial impact on one of the Parties. Contractor's failure to meet a Quarterly Milestone is considered a Type 1 Dispute. In addition, any Dispute that impacts Contractor's timing or amount of a Quality Maintenance Payment, as defined in **Exhibit E**, Compensation and Quality Maintenance Payments, is considered a Type 1 Dispute.

b. Type 2 Disputes are ones that are considered less severe than a Type 1 Dispute or do not have a direct financial impact on either Party. Any Dispute not considered a Type 1 Dispute is a Type 2 Dispute.

ii. The State and Contractor are expected to resolve Disputes at the lowest level possible and as quickly as possible to maintain a positive working relationship and maintain the timeline for implementation of the PBMS. If the Dispute cannot be resolved, the Parties shall escalate the dispute in the following manner:

a. Level 1: The Dispute will be discussed and resolved by the representatives described in section 16. If the Dispute is not resolved at this level, the Parties shall escalate it to Level 2. During the PBMS Implementation Contract Stage, this process will take no longer than ten (10) Business Days for Type 2 Disputes and five (5) Business Days for Type 1 Disputes.

b. Level 2: The Dispute will be discussed and resolved by the Executive Director of the Department or his or her written Designee and the Chief Executive Officer of Contractor or his or her written Designee. Should the Dispute not be resolved at this level, the Parties will escalate it to Level 3. During the PBMS Implementation Contract Stage, this process will take no longer than twenty (20) additional Business Days for Type 2 Disputes and ten (10) Business Days for Type 1 Disputes.

c. Level 3: Any Dispute unresolved in Level 1 and 2 will be escalated to a mediator of the Mediation Center of Colorado or such other mediation provider as may be agreed. Each Party will choose an eligible mediator. Those two individuals will select a third individual to act as a mediator for this Dispute. The Parties will share the cost of the mediator equally. He or she will engage both parties in mediation in Denver, Colorado. During the PBMS Implementation Contract Stage, this process will take no longer than twenty (20) additional Business Days for Type 2 Disputes and ten (10) Business Days for Type 1 Disputes.

d. During the PBMS Ongoing Operations and Enhancements Contract Stage, the time to escalate a Dispute from Level 1 to Level 2 to Level 3 may be modified through a Contract amendment, if a longer period to resolve Disputes prior to mediation is desired by both parties.

e. To initiate the Dispute Process, one of the representatives described in section 16 must issue a notice to the other in writing, as defined in the Communication Management Plan, as defined in **Exhibit C**, Requirements.

iii. The Dispute Process is available to both Parties and, subject to the limitations set forth below, it shall be used to resolve all issues that arise under this Contract including, but not limited to:
   a. All contract requirements covered in the Contract.
   b. The payment of Quality Maintenance Payments.
   c. Assessment and calculation of liquidated damages.
   d. Withholding or denial of payment.
   e. Removal of a Key Personnel or Subcontractors under the Contract.
   f. Termination for cause and/or breach or early termination in the public interest.
   g. Contractor's failure to perform its responsibilities, which may or may not impact Quality Maintenance Payments or Performance Standards, as defined in **Exhibit G**, if such failure is the result of the State's or its agent's failure to perform its functions or obligations under the Contract.

iv. The Parties agree that they will participate in the Dispute Process in good faith and will attempt to resolve Disputes as quickly as possible. Except for situations where equitable relief is necessary to prevent irreparable harm, the Parties will complete the Dispute Process before initiating any legal action to resolve the Dispute. If equitable relief is necessary to prevent irreparable harm a Party may proceed with a legal action to seek such relief without completing or participating in the Dispute Process. For avoidance of doubt, any breach of obligations with respect to Confidential Information or personal information shall be deemed to cause irreparable harm and a Party may immediately seek equitable relief without the necessity of showing irreparable harm or posting bond.

v. Continued Performance.
   Except where clearly prevented by the area in dispute, both Parties shall continue performing their obligations under this Contract while the dispute is being resolved under this Section 20.E unless and until the dispute is resolved or until this Contract is terminated. The time frame to cure any breach of the terms of this Contract shall not be tolled by the pendency of any dispute resolution procedures.

F. Lobbying

Contractor certifies, to the best of its knowledge and belief, that:

i. No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any Federal grant, the making of any federal loan, the entering into of any cooperative Contract, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative contract.

ii. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an office or employee of any agency, a Member of Congress, an office or employee of Congress, or an employee of a Member of Congress in connection with this

federal contract, grant, loan, or cooperative Contract, Contractor shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

iii. Contractor shall require that the language of this certification be included in the award documents for all sub awards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative Contracts) and that all subrecipients shall certify and disclose accordingly.

iv. This certification is a material representation of fact upon which reliance was placed when the transaction was made or entered into. Submission of the certification is a requisite for making or entering into transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000.00 and not more than $100,000.00 for each such failure.

G. Cyber Security Requirements.

The following obligations shall apply with respect to this Contract.

i. Protection.

a. If Contractor or any of its Subcontractors provide physical or logical storage, processing or transmission of Confidential Information, Contractor shall provide, and shall cause its Subcontractors to provide, physical and logical protection for Confidential Information while in Contractor's possession or control that meets or exceeds the standards identified in **Exhibit H**, State Cybersecurity Policies and the requirements set forth in this Contract. Contractor shall provide the State with reasonable access, subject to Contractor's reasonable access security requirements and reasonable notice, for the purpose of inspecting and monitoring access and use of data, and evaluating physical and logical security control effectiveness.

b. Contractor shall at all times maintain, and shall cause its Subcontractors to maintain, network, system, and application security, which includes network firewalls, intrusion detection, and annual security testing required by the Colorado Office of Information Security within the Governor's Office of Information Technology ("OIS"). All Confidential Information shall be stored, processed, or transferred only in or to facilities located within the United States. Contractor shall comply, and shall cause its Subcontractors to comply, with applicable State and federal regulations and guidelines related to security, confidentiality and auditing. Without limiting the foregoing, Contractor shall implement and maintain, and shall cause its Subcontractors to implement, monitor and maintain, network, system and application security measures meeting or exceeding the standards, as identified in **Exhibit H**, State Cybersecurity Policies. Contractor shall develop, as part of the System Security Plan, a process to define and promptly report breaches or attempted breaches of network, system, or application security to a representative of the OIS and the State.

c. Contractor shall review, on a semi-annual basis, the Colorado Cyber Security Program (CCSP), posted at:

http://www.colorado.gov/cs/Satellite/Cyber/CSIO/1207820732279 (or any successor web site thereto), and its related documents, including its policies and procedures to ensure compliance with the standards and guidelines published therein, such that changes may be implemented through the Change Management Process.

d. Contractor shall reasonably cooperate, and shall cause its Subcontractors to cooperate, with the performance of security audit and penetration tests by OIS, which tests can be done not more often than one (1) time in any rolling six (6) month period. Contractor shall follow the State's Data Handling and Disposal policy, which is attached as **Exhibit H**, State Cybersecurity Policies. Contractor shall perform or shall have had performed, and shall cause its Subcontractors to perform background checks on all of its respective employees and agents performing onsite Services or having access to Confidential Information.

ii. Security Notice.

Contractor is responsible for the security of all data and information provided to it by the State while any such data and information is in Contractor's possession or control. Contractor shall comply, and shall cause its Subcontractors to comply, with the State's Cyber Security Policies, which are attached as **Exhibit H**, State Cybersecurity Policies.

iii. Security Breach Remediation.

In the case of any security breach or unauthorized access to or use of any Personal Identifying Information, as defined in CRS § 18-5-901 (13), Contractor and any Subcontractor will comply with Colorado's Consumer Protection Law.

21. COLORADO SPECIAL PROVISIONS

The Special Provisions apply to all contracts except where noted in *italics*.

A. **CONTROLLER'S APPROVAL**. **CRS §24-30-202(1)**. This Contract shall not be valid until it has been approved by the Colorado State Controller or designee.

B. **FUND AVAILABILITY**. **CRS §24-30-202(5.5)**. Financial obligations of the State payable after the current Fiscal Year are contingent upon funds for that purpose being appropriated, budgeted, and otherwise made available.

C. **GOVERNMENTAL IMMUNITY**. No term or condition of this Contract shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protections, or other provisions, of the Colorado Governmental Immunity Act, CRS §24-10-101 *et seq*., or the Federal Tort Claims Act, 28 U.S.C. §§1346(b) and 2671 *et seq*., as applicable now or hereafter amended.

D. **INDEPENDENT CONTRACTOR**. Contractor shall perform its duties hereunder as an independent contractor and not as an employee. Neither Contractor nor any agent or employee of Contractor shall be deemed to be an agent or employee of the State. Contractor and its employees and agents are not entitled to unemployment insurance or workers compensation benefits through the State and the State shall not pay for or otherwise provide such coverage for Contractor or any of its agents or employees. Unemployment insurance benefits will be available to Contractor and its employees and agents only if such coverage is made available by Contractor or a third party. Contractor shall pay when due all applicable employment taxes and

income taxes and local head taxes incurred pursuant to this Contract. Contractor shall not have Authorization, express or implied, to bind the State to any agreement, liability or understanding, except as expressly set forth herein. Contractor shall **(a)** provide and keep in force workers' compensation and unemployment compensation insurance in the amounts required by law, **(b)** provide proof thereof when requested by the State, and **(c)** be solely responsible for its acts and those of its employees and agents.

E. **COMPLIANCE WITH LAW**. Contractor shall strictly comply with all applicable federal and State laws, rules, and regulations in effect or hereafter established, including, without limitation, laws applicable to discrimination and unfair employment practices.

F. **CHOICE OF LAW**. Colorado law, and rules and regulations issued pursuant thereto, shall be applied in the interpretation, execution, and enforcement of this Contract. Any provision included or incorporated herein by reference which conflicts with said laws, rules, and regulations shall be null and void. Any provision incorporated herein by reference which purports to negate this or any other Special Provision in whole or in part shall not be valid or enforceable or available in any action at law, whether by way of complaint, defense, or otherwise. Any provision rendered null and void by the operation of this provision shall not invalidate the remainder of this Contract, to the extent capable of execution.

G. **BINDING ARBITRATION PROHIBITED.** The State of Colorado does not agree to binding arbitration by any extra-judicial body or person. Any provision to the contrary in this Contract or incorporated herein by reference shall be null and void.

H. **SOFTWARE PIRACY PROHIBITION. Governor's Executive Order D00200**. State or other public funds payable under this Contract shall not be used for the acquisition, operation, or Maintenance of computer software in violation of federal copyright laws or applicable licensing restrictions. Contractor hereby certifies and warrants that, during the term of this Contract and any extensions, Contractor has and shall maintain in place appropriate systems and controls to prevent such improper use of public funds. If the State determines that Contractor is in violation of this provision, the State may exercise any remedy available at law or in equity or under this Contract, including, without limitation, immediate termination of this Contract and any remedy consistent with federal copyright laws or applicable licensing restrictions.

I. **EMPLOYEE FINANCIAL INTEREST/CONFLICT OF INTEREST**. **CRS §§24-18-201 and 24-50-507**. The signatories aver that to their knowledge, no employee of the State has any personal or beneficial interest whatsoever in the service or property described in this Contract. Contractor has no interest and shall not acquire any interest, direct or indirect, that would conflict in any manner or degree with the performance of Contractor's services and Contractor shall not employ any person having such known interests.

J. **VENDOR OFFSET**. **CRS §§24-30-202 (1) and 24-30-202.4**. [***Not Applicable to intergovernmental agreements***] Subject to CRS §24-30-202.4 (3.5), the State Controller may withhold payment under the State's vendor offset intercept system for debts owed to State agencies for: **(a)** unpaid child support debts or child support arrearages; **(b)** unpaid balances of tax, accrued interest, or other charges

specified in CRS §39-21-101, *et seq*.; **(c)** unpaid loans due to the Student Loan Division of the Department of Higher Education; **(d)** amounts required to be paid to the Unemployment Compensation Fund; and **(e)** other unpaid debts owing to the State as a result of final agency determination or judicial action.

K. **PUBLIC CONTRACTS FOR SERVICES. CRS §8-17.5-101.** ***[Not Applicable to agreements relating to the offer, issuance, or sale of securities, investment advisory services or fund management services, sponsored projects, intergovernmental agreements, or information technology services or products and services]*** Contractor certifies, warrants, and agrees that it does not knowingly employ or contract with an illegal alien who will perform work under this Contract and will confirm the employment eligibility of all employees who are newly hired for employment in the United States to perform work under this Contract, through participation in the E-Verify Program or the Department program established pursuant to CRS §8-17.5-102(5)(c), Contractor shall not knowingly employ or contract with an illegal alien to perform work under this Contract or enter into a contract with a subcontractor that fails to certify to Contractor that the subcontractor shall not knowingly employ or contract with an illegal alien to perform work under this Contract. Contractor (a) shall not use E-Verify Program or Department program procedures to undertake pre-employment screening of job applicants while this Contract is being performed, (b) shall notify the subcontractor and the contracting State agency within three days if Contractor has actual knowledge that a subcontractor is employing or contracting with an illegal alien for work under this Contract, (c) shall terminate the subcontract if a subcontractor does not stop employing or contracting with the illegal alien within three days of receiving the notice, and (d) shall comply with reasonable requests made in the course of an investigation, undertaken pursuant to CRS §8-17.5-102(5), by the Colorado Department of Labor and Employment. If Contractor participates in the Department program, Contractor shall deliver to the contracting State agency, Institution of Higher Education or political subdivision a written, notarized affirmation, affirming that Contractor has examined the legal work status of such employee, and shall comply with all of the other requirements of the Department program. If Contractor fails to comply with any requirement of this provision or CRS §8-17.5-101 *et seq*., the contracting State agency, institution of higher education or political subdivision may terminate this Contract for breach and, if so terminated, Contractor shall be liable for damages.

L. **PUBLIC CONTRACTS WITH NATURAL PERSONS. CRS §24-76.5-101.** Contractor, if a natural person eighteen (18) years of age or older, hereby swears and affirms under penalty of perjury that he or she **(a)** is a citizen or otherwise lawfully present in the United States pursuant to federal law, **(b)** shall comply with the provisions of CRS §24-76.5-101 *et seq.*, and **(c)** has produced one form of identification required by CRS §24-76.5-103 prior to the effective date of this contract.

Contract Routing Number 201500002104

SIGNATURE PAGE

THE PARTIES HERETO HAVE EXECUTED THIS CONTRACT

*** Persons signing for Contractor hereby swear and affirm that they are authorized to act on Contractor's behalf and acknowledge that the State is relying on their representations to that effect.**

CONTRACTOR
Magellan Medicaid Administration, Inc.

_____
***Signature**

Date: 9/4/2015

By: GREGORY S. KAUFF
Name of Authorized Individual

Title: SVP/General Manager Govt Mkts
Official Title of Authorized Individual

STATE OF COLORADO
John W. Hickenlooper, Governor
Department of Health Care Policy and Financing

_____
Susan E. Birch, MBA, BSN, RN
Executive Director
Signatory avers to the State Controller or delegate that Contractor has not begun performance or that a Statutory Violation waiver has been requested under Fiscal Rules

Date: 9/11/2015

LEGAL REVIEW
Cynthia H. Coffman, Attorney General

By: N/A
Signature - Assistant Attorney General

Date: _____

ALL CONTRACTS REQUIRE APPROVAL BY THE STATE CONTROLLER

CRS §24-30-202 requires the State Controller to approve all State Contracts. This Contract is not valid until signed and dated below by the State Controller or delegate. Contractor is not authorized to begin performance until such time. If Contractor begins performing prior thereto, the State of Colorado is not obligated to pay Contractor for such performance or for any goods and/or services provided hereunder.

STATE CONTROLLER
Robert Jaros, CPA, MBA, JD

By: _____
Department of Health Care Policy and Financing

Date: 9/24/15

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum ("Addendum") is part of the Contract between the State of Colorado, Department of Health Care Policy and Financing and Contractor. For purposes of this Addendum, the State is referred to as "Department", "Covered Entity" or "CE" and Contractor is referred to as "Associate". Unless the context clearly requires a distinction between the Contract document and this Addendum, all references herein to "the Contract" or "this Contract" include this Addendum.

RECITALS

A. CE wishes to disclose certain information to Associate pursuant to the terms of the Contract, some of which may constitute Protected Health Information ("PHI") (defined below).

B. CE and Associate intend to protect the privacy and provide for the security of PHI disclosed to Associate pursuant to this Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §1320d – 1320d-8 ("HIPAA") as amended by the American Recovery and Reinvestment Act of 2009 ("ARRA")/HITECH Act (P.L. 111-005), and its implementing regulations promulgated by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160, 162 and 164 (the "Privacy Rule") and other applicable laws, as amended.

C. As part of the HIPAA regulations, the Privacy Rule requires CE to enter into a contract containing specific requirements with Associate prior to disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 160.103, 164.502(e) and 164.504(e) of the Code of Federal Regulations ("C.F.R.") and contained in this Addendum.

The parties agree as follows:

1. Definitions.

a. Except as otherwise defined herein, capitalized terms in this Addendum shall have the definitions set forth in the HIPAA Privacy Rule at 45 C.F.R. Parts 160, 162 and 164, as amended. In the event of any conflict between the mandatory provisions of the Privacy Rule and the provisions of this Contract, the Privacy Rule shall control. Where the provisions of this Contract differ from those mandated by the Privacy Rule, but are nonetheless permitted by the Privacy Rule, the provisions of this Contract shall control.

b. "Protected Health Information" or "PHI" means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

c. "Protected Information" shall mean PHI provided by CE to Associate or created or received by Associate on CE's behalf. To the extent Associate is a covered entity under HIPAA and creates or obtains its own PHI for treatment, payment and health care operations, Protected Information under this Contract does not include any PHI created or obtained by Associate as a covered entity and Associate shall follow its own policies and procedures for accounting, access and amendment of Associate's PHI.

2. Obligations of Associate.

a. Permitted Uses. Associate shall not use Protected Information except for the purpose of performing Associate's obligations under this Contract and as permitted under this Addendum. Further, Associate shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule if so used by CE, except that Associate may use Protected

Information: (i) for the proper management and administration of Associate; (ii) to carry out the legal responsibilities of Associate; or (iii) for Data Aggregation purposes for the Health Care Operations of CE. Additional provisions, if any, governing permitted uses of Protected Information are set forth in Attachment A to this Addendum. Associate accepts full responsibility for any penalties incurred as a result of Associate's breach of the Privacy Rule.

b. Permitted Disclosures. Associate shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule if disclosed by CE, except that Associate may disclose Protected Information: (i) in a manner permitted pursuant to this Contract; (ii) for the proper management and administration of Associate; (iii) as required by law; (iv) for Data Aggregation purposes for the Health Care Operations of CE; or (v) to report violations of law to appropriate federal or state authorities, consistent with 45 C.F.R. Section 164.502(j)(1). To the extent that Associate discloses Protected Information to a third party, Associate must obtain, prior to making any such disclosure: (i) reasonable assurances from such third party that such Protected Information will be held confidential as provided pursuant to this Addendum and only disclosed as required by law or for the purposes for which it was disclosed to such third party; and (ii) an agreement from such third party to notify Associate within two Business Days of any breaches of confidentiality of the Protected Information, to the extent it has obtained knowledge of such breach. Additional provisions, if any, governing permitted disclosures of Protected Information are set forth in Attachment A.

c. Appropriate Safeguards. Associate shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by this Contract. Associate shall comply with the requirements of the Security Rules, 164.308, 164.310, 164.312, and 164.316. Associate shall maintain a comprehensive written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Associate's operations and the nature and scope of its activities.

d. Reporting of Improper Use or Disclosure. Associate shall report to CE in writing any use or disclosure of Protected Information other than as provided for by this Contract within five (5) Business Days of becoming aware of such use or disclosure.

e. Associate's Agents. If Associate uses one or more subcontractors or agents to provide services under the Contract, and such subcontractors or agents receive or have access to Protected Information, each subcontractor or agent shall sign an agreement with Associate containing substantially the same provisions as this Addendum and further identifying CE as a third party beneficiary with rights of enforcement and indemnification from such subcontractors or agents in the event of any violation of such subcontractor or agent agreement. Associate shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions shall mitigate the effects of any such violation.

f. Access to Protected Information. Associate shall make Protected Information maintained by Associate or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying within ten (10) Business Days of a request by CE to enable CE to fulfill its obligations to permit individual access to PHI under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524.

g. Amendment of PHI. Within ten (10) Business Days of receipt of a request from CE for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, Associate or its agents or subcontractors shall make such Protected Information available to CE for amendment and incorporate any such amendment to enable CE to fulfill its obligations with respect to requests by individuals to amend their PHI under the Privacy

Rule, including, but not limited to, 45 C.F.R. Section 164.526. If any individual requests an amendment of Protected Information directly from Associate or its agents or subcontractors, Associate must notify CE in writing within five (5) Business Days of receipt of the request. Any denial of amendment of Protected Information maintained by Associate or its agents or subcontractors shall be the responsibility of CE.

h. Accounting Rights. Within ten (10) Business Days of notice by CE of a request for an accounting of disclosures of Protected Information, Associate and its agents or subcontractors shall make available to CE the information required to provide an accounting of disclosures to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.528. As set forth in, and as limited by, 45 C.F.R. Section 164.528, Associate shall not provide an accounting to CE of disclosures: (i) to carry out treatment, payment or health care operations, as set forth in 45 C.F.R. Section 164.506; (ii) to individuals of Protected Information about them as set forth in 45 C.F.R. Section 164.502; (iii) pursuant to an Authorization as provided in 45 C.F.R. Section 164.508; (iv) to persons involved in the individual's care or other notification purposes as set forth in 45 C.F.R. Section 164.510; (v) for national security or intelligence purposes as set forth in 45 C.F.R. Section 164.512(k)(2); (vi) to correctional institutions or law enforcement officials as set forth in 45 C.F.R. Section 164.512(k)(5); (vii) incident to a use or disclosure otherwise permitted by the Privacy Rule; (viii) as part of a limited data set under 45 C.F.R. Section 164.514(e); or (ix) disclosures prior to April 14, 2003. Associate agrees to implement a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years prior to the request, but not before the compliance date of the Privacy Rule. At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's Authorization, or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to Associate or its agents or subcontractors, Associate shall within five (5) Business Days of the receipt of the request forward it to CE in writing. It shall be CE's responsibility to prepare and deliver any such accounting requested. Associate shall not disclose any Protected Information except as set forth in Section 2(b) of this Addendum.

i. Governmental Access to Records. Associate shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary"), in a time and manner designated by the Secretary, for purposes of determining CE's compliance with the Privacy Rule. Associate shall provide to CE a copy of any Protected Information that Associate provides to the Secretary concurrently with providing such Protected Information to the Secretary.

j. Minimum Necessary. Associate (and its agents or subcontractors) shall only request, use and disclose the minimum amount of Protected Information necessary to accomplish the purpose of the request, use or disclosure, in accordance with the Minimum Necessary requirements of the Privacy Rule including, but not limited to, 45 C.F.R. Sections 164.502(b) and 164.514(d).

k. Data Ownership. Associate acknowledges that Associate has no ownership rights with respect to the Protected Information.

l. Retention of Protected Information. Except upon termination of the Contract as provided in Section 4(d) of this Addendum, Associate and its agents or subcontractors shall retain all Protected Information throughout the term of this Contract and shall continue to maintain the information required under Section 2(h) of this Addendum for a period of six (6) years.

m. Associate's Insurance. Associate shall maintain casualty and liability insurance to cover loss of PHI data and claims based upon alleged violations of privacy rights through improper use or disclosure of PHI. All such policies shall meet or exceed the minimum insurance requirements of the Contract (e.g., occurrence basis, combined single dollar limits, annual aggregate dollar limits, additional insured status and notice of cancellation).

n. Notification of Breach. During the term of this Contract, Associate shall notify CE within two (2) Business Days of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired or disclosed during the breach. Associate shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

o. Audits, Inspections and Enforcement. Within ten (10) Business Days of a written request by CE, Associate and its agents or subcontractors shall allow CE to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of Protected Information pursuant to this Addendum for the purpose of determining whether Associate has complied with this Addendum; provided, however, that: (i) Associate and CE shall mutually agree in advance upon the scope, timing and location of such an inspection; (ii) CE shall protect the confidentiality of all confidential and proprietary information of Associate to which CE has access during the course of such inspection; and (iii) CE shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Associate. The fact that CE inspects, or fails to inspect, or has the right to inspect, Associate's facilities, systems, books, records, agreements, policies and procedures does not relieve Associate of its responsibility to comply with this Addendum, nor does CE's (i) failure to detect or (ii) detection, but failure to notify Associate or require Associate's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of CE's enforcement rights under the Contract.

p. Safeguards During Transmission. Associate shall be responsible for using appropriate safeguards to maintain and ensure the confidentiality, privacy and security of Protected Information transmitted to CE pursuant to the Contract, in accordance with the standards and requirements of the Privacy Rule, until such Protected Information is received by CE, and in accordance with any Specifications set forth in Attachment A.

q. Restrictions and Confidential Communications. Within ten (10) Business Days of notice by CE of a restriction upon uses or disclosures or request for confidential communications pursuant to 45 C.F.R. Section 164.522, Associate will restrict the use or disclosure of an individual's Protected Information, provided Associate has agreed to such a restriction. Associate will not respond directly to an individual's requests to restrict the use or disclosure of Protected Information or to send all communication of Protected Information to an alternate address. Associate will refer such requests to the CE so that the CE can coordinate and prepare a timely response to the requesting individual and provide direction to Associate.

3. Obligations of CE.

a. Safeguards During Transmission. CE shall be responsible for using appropriate safeguards to maintain and ensure the confidentiality, privacy and security of PHI transmitted to Associate pursuant to this Contract, in accordance with the standards and requirements of the Privacy Rule, until such PHI is received by Associate, and in accordance with any Specifications set forth in Attachment A.

b. Notice of Changes. CE shall provide Associate with a copy of its notice of privacy practices produced in accordance with 45 C.F.R. Section 164.520, as well as any subsequent changes or limitation(s) to such notice, to the extent such changes or limitation(s) may affect Associate's use or disclosure of Protected Information. CE shall provide Associate with any changes in, or revocation of, permission to use or disclose Protected Information, to the extent it may affect Associate's permitted use or disclosure of PHI, CE shall notify Associate of any restriction on the use or disclosure of Protected Information that CE has agreed to in accordance with 45 C.F.R. Section 164.522. CE may effectuate any and all such notices of non-private information via posting on CE's web site. Associate shall review CE's designated web site for notice of changes to CE's HIPAA privacy policies and practices on the last day of each calendar quarter.

4. Termination.

a. Material Breach. In addition to any other provisions in the Contract regarding breach, a breach by Associate of any provision of this Addendum, as determined by CE, shall

constitute a material breach of this Contract and shall provide grounds for immediate termination of this Contract by CE pursuant to the provisions of the Contract covering termination for cause, if any. If the Contract contains no express provisions regarding termination for cause, the following terms and conditions shall apply:

(1) Default. If Associate refuses or fails to timely perform any of the provisions of this Contract, CE may notify Associate in writing of the non-performance, and if not promptly corrected within the time specified, CE may terminate this Contract. Associate shall continue performance of this Contract to the extent it is not terminated and shall be liable for excess costs incurred in procuring similar goods or services elsewhere.

(2) Associate's Duties. Notwithstanding termination of this Contract, and subject to any directions from CE, Associate shall take timely, reasonable and necessary action to protect and preserve property in the possession of Associate in which CE has an interest.

(3) Compensation. Payment for completed supplies delivered and accepted by CE shall be at the Contract price. In the event of a material breach under paragraph 4(a), CE may withhold amounts due Associate as CE deems necessary to protect CE against loss from third party claims of improper use or disclosure and to reimburse CE for the excess costs incurred in procuring similar goods and services elsewhere.

(4) Erroneous Termination for Default. If after such termination it is determined, for any reason, that Associate was not in default, or that Associate's action/inaction was excusable, such termination shall be treated as a termination for the public interest, and the rights and obligations of the parties shall be the same as if this Contract had been terminated for the public interest, as described in this Contract.

b. Reasonable Steps to Cure Breach. If CE knows of a pattern of activity or practice of Associate that constitutes a material breach or violation of the Associate's obligations under the provisions of this Addendum or another arrangement and does not terminate this Contract pursuant to Section 4(a), then CE shall take reasonable steps to cure such breach or end such violation, as applicable. If CE's efforts to cure such breach or end such violation are unsuccessful, CE shall either (i) terminate the Contract, if feasible or (ii) if termination of this Contract is not feasible, CE shall report Associate's breach or violation to the Secretary of the Department of Health and Human Services.

c. Judicial or Administrative Proceedings. Either party may terminate the Contract, effective immediately, if (i) the other party is named as a defendant in a criminal proceeding for a violation of HIPAA, the HIPAA Regulations or other security or privacy laws or (ii) a finding or stipulation that the other party has violated any standard or requirement of HIPAA, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.

d. Effect of Termination.

(1) Except as provided in paragraph (2) of this subsection, upon termination of this Contract, for any reason, Associate shall return or destroy all Protected Information that Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information that Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected information. If Associate elects to destroy the PHI, Associate shall certify in writing to CE that such PHI has been destroyed.

(2) If Associate believes that returning or destroying the Protected Information is not feasible, Associate shall promptly provide CE notice of the conditions making return or destruction infeasible. Upon mutual agreement of CE and Associate that return or destruction of Protected Information is infeasible, Associate shall continue to extend the protections of Sections 2(a), 2(b), 2(c), 2(d) and 2(e) of this Addendum to such information, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible.

5. Injunctive Relief. CE shall have the right to injunctive and other equitable and legal relief against Associate or any of its agents or subcontractors in the event of any use or disclosure of Protected Information in violation of this Contract or applicable law.

6. No Waiver of Immunity. No term or condition of this Contract shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions of the Colorado Governmental Immunity Act, CRS 24-10-100 *et seq*. or the Federal Tort Claims Act, 28 U.S.C. 2671 *et seq*. as applicable, as now in effect or hereafter amended.

7. Limitation of Liability. Any limitation of Associate's liability in the Contract shall be inapplicable to the terms and conditions of this Addendum.

8. Disclaimer. CE makes no warranty or representation that compliance by Associate with this Contract, HIPAA or HIPAA Regulations will be adequate or satisfactory for Associate's own purposes. Associate is solely responsible for all decisions made by Associate regarding the safeguarding of PHI.

9. Certification. To the extent that CE determines an examination is necessary in order to comply with CE's legal obligations pursuant to HIPAA relating to certification of its security practices, CE or its authorized agents or contractors may, at CE's expense, examine Associate's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to CE the extent to which Associate's security safeguards comply with HIPAA, the HIPAA Regulations or this Addendum.

10. Amendment.

a. Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The Parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the Privacy Rule, the Final HIPAA Security Regulations at 68 Fed. Reg. 8334 (Feb 20, 2003), 45 C.F.R. §164.314 and other applicable laws relating to the security or privacy of PHI. The parties understand and agree that CE must receive satisfactory written assurance from Associate that Associate will adequately safeguard all Protected

Information. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the Privacy Rule or other applicable laws. CE may terminate this Contract upon thirty (30) days written notice in the event (i) Associate does not promptly enter into negotiations to amend this Contract when requested by CE pursuant to this Section or (ii) Associate does not enter into an amendment to this Contract providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the Privacy Rule.

b. Amendment of Attachment A. Attachment A may be modified or amended by mutual agreement of the parties in writing from time to time without formal amendment of this Addendum.

11. Assistance in Litigation or Administrative Proceedings. Associate shall make itself, and any subcontractors, employees or agents assisting Associate in the performance of its obligations under the Contract, available to CE, at no cost to CE, up to a maximum of thirty (30) hours, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers or employees based upon a claimed violation of HIPAA, the Privacy Rule or other laws relating to security and privacy or PHI, except where Associate or its subcontractor, employee or agent is a named adverse party.

12. No Third Party Beneficiaries. Nothing express or implied in this Contract is intended to confer, nor shall anything herein confer, upon any person other than CE, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

13. Interpretation and Order of Precedence. The provisions of this Addendum shall prevail over any provisions in the Contract that may conflict or appear inconsistent with any provision in this Addendum. Together, the Contract and This Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA and the Privacy Rule. The parties agree that any ambiguity in this Contract shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the Privacy Rule. This Contract supersedes and replaces any previous separately executed HIPAA addendum between the parties.

14. Survival of Certain Contract Terms. Notwithstanding anything herein to the contrary, Associate's obligations under Section 4(d) ("Effect of Termination") and Section 12 ("No Third Party Beneficiaries") shall survive termination of this Contract and shall be enforceable by CE as provided herein in the event of such failure to perform or comply by the Associate. This Addendum shall remain in effect during the term of the Contract including any extensions.

ATTACHMENT A

This Attachment sets forth additional terms to the HIPAA Business Associate Addendum, which is part of the Contract between the State of Colorado, Department of Health Care Policy and Financing and Contractor and is effective as of the date of the Contract (the "Attachment Effective Date"). This Attachment may be amended from time to time as provided in Section 10(b) of the Addendum.

1. Additional Permitted Uses. In addition to those purposes set forth in Section 2(a) of the Addendum, Associate may use Protected Information as follows:

No additional permitted uses.

2. Additional Permitted Disclosures. In addition to those purposes set forth in Section 2(b) of the Addendum, Associate may disclose Protected Information as follows:

No additional permitted disclosures.

3. Subcontractor(s). The parties acknowledge that the following subcontractors or agents of Associate shall receive Protected Information in the course of assisting Associate in the performance of its obligations under this Contract:

Contractor will notify the State of any proposed subcontractor or agent before providing access to PHI as required by the Contract.

4. Receipt. Associate's receipt of Protected Information pursuant to this Contract shall be deemed to occur as follows and Associate's obligations under the Addendum shall commence with respect to such PHI upon such receipt:

Upon receipt of PHI from the Department.

5. Additional Restrictions on Use of Data. CE is a Business Associate of certain other Covered Entities and, pursuant to such obligations of CE, Associate shall comply with the following restrictions on the use and disclosure of Protected Information:

No Additional Restrictions.

6. Additional Terms. [Section may include Specifications for disclosure format, method of transmission, use of an intermediary, use of digital signatures or PKI, authentication, additional security or privacy Specifications, de-identification/re-identification of data, etc.]:

No additional terms.

EXHIBIT A, STATEMENT OF WORK

1. CONTRACT STAGES AND PROJECT PHASES

1.1. Contract Stages

1.1.1. All of the following stages shall be part of this Contract:

1.1.1.1. PBMS Implementation Contract Stage.

1.1.1.1.1. The PBMS Implementation Contract Stage shall include all of the following:

1.1.1.1.1.1. Replacing the Department's existing pharmacy benefits management services functionality within its MMIS with a new PBMS designed, developed and implemented by the Contractor.

1.1.1.1.1.2. Completing all activities associated with the integration of the PBMS with the new MMIS functionality.

1.1.1.1.1.3. Implementing all activities associated with performing PBMS functions, including, but not limited to, operating and maintaining the PBMS and performing upgrades as required.

1.1.1.1.2. The intent of the PBMS Implementation Contract Stage is to limit disruption in program services, to the greatest practical extent and improve the Department's understanding of the Contractor's PBMS and Services by providing overview training to the appropriate Department personnel.

1.1.1.2. PBMS Ongoing Operations and Enhancement Contract Stage.

1.1.1.2.1. The PBMS Ongoing Operations and Enhancement Stage shall include all of the following:

1.1.1.2.1.1. Operate and maintain the PBMS after it is implemented by the Contractor.

1.1.1.2.1.2. Providing all Services required to support the PBMS and PBMS system users.

1.1.1.2.1.3. Enhance the PBMS to improve operations.

1.1.1.2.2. The intent of the PBMS Ongoing Operations and Enhancements Contract Stage is to improve the PBMS with Enhancements that will address the various business processes, improve enterprise integration, and focus on integration with data analytics tools to improve the management of patient outcomes.

1.1.1.2.3. The PBMS Ongoing Operations and Enhancement Contract Stage shall include separate years in which this Contract Stage occurs.

1.1.1.2.4. The first year of the PBMS Ongoing Operations and Enhancement Contract Stage shall begin as specified in the most recently approved Project Management Plan. Each subsequent year of the PBMS Ongoing Operations and Enhancement Contract Stage shall begin annually as defined in the Project Management Plan.

1.1.2. Each Contract Stage shall not begin until the entrance criteria for the Project Phases in Exhibit D contained in that Contract Stage have been met. Each Contract Stage shall only end once all exit criteria for the Project Phases in Exhibit D contained in that Contract Stage have been met and all requirements in Exhibit C for that Contract Stage have been completed.

1.1.2.1. Any stage may occur concurrently with any other stage based on the timelines, entry and exit criteria, and requirements for each stage.

1.1.2.2. Each Contract Stage will begin and end on the dates contained in the most recently approved Project Management Plan.

1.2. Project Phases

1.2.1. This Contract shall include all Project Phases included in Exhibit D.

1.2.1.1. All entrance and exit criteria listed for a Project Phase in Exhibit D shall be completed. It may be completed in a staggered fashion for development components as described in the Project Management Plan.

1.2.2. During each Project Phase, the Contractor shall perform all Contractor responsibilities listed for that Project Phase in Exhibit D.

2. REQUIREMENT COMPLIANCE

2.1. In addition to all requirements described in this Statement of Work, the Contractor shall comply with all requirements contained in Exhibit C, Requirements.

2.1.1. The Contractor shall comply with each requirement listed in Exhibit C during the Contract Stage or stages noted in that requirement. A requirement shall be implemented in the stage provided in Exhibit C for that requirement. Once a requirement is implemented, the Contractor shall comply with ongoing responsibilities to maintain the implemented requirement in all future stages.

2.1.2. The Contractor shall meet all performance standards contained in Exhibit E and Exhibit G.

2.1.3. Contractor's Approach

2.1.3.1. The Contractor's Approach provides a general description of how the Contractor will comply with each requirement in Exhibit C. This section is not intended to be exhaustive of how the Contractor will comply with the requirement and shall not limit the Contractor's responsibility to comply with any requirement.

2.1.3.2. For any requirement where the Contractor's approach requires approval from the Department, the Contractor shall implement that requirement as proposed by the Contractor and approved by the Department.

2.1.3.3. In the event that the Contractor determines that a different approach is necessary for a requirement, the Contractor shall propose to the Department how it will modify its approach through the Change Management Process.

2.1.3.4. If a Contractor's approach to meeting a requirement includes the use of a specific system or software, the Contractor may use a different system or software that

provides the same functionality to meet that requirement upon written approval of the Department.

2.1.4. For each requirement in Exhibit C that requires the Contractor to create, establish, develop, compile or prepare any document, plan or deliverable, the document, plan or deliverable shall be considered a document deliverable, as described in section 5.1 of this Statement of Work and shall be subject to all deliverable submission and acceptance requirements described in that section.

3. LOCATION OF CONTRACT FUNCTIONS

3.1. In no event shall the Contractor perform any Work outside of the United States or its territories. At no time shall the Contractor maintain, use, transmit, or cause to be transmitted information governed by privacy laws and regulations outside the United States and its territories.

4. CONTRACT PERSONNEL

4.1. The Contractor shall develop and maintain appropriate staffing levels throughout the term of this Contract and shall adjust its resources, as necessary, to maintain compliance with all requirements of this Contract.

4.2. The Contractor shall provide at least two (2) FTEs to provide four-thousand, one-hundred and sixty (4,160) hours of Customization work under this Contract on an annual basis during the Ongoing Operation and Enhancement Contract Stage. In addition, the Contractor shall provide least two (2) FTEs to provide four-thousand, one-hundred and sixty (4,160) hours of Configuration work under this Contract on an annual basis during the Ongoing Operation and Enhancement Contract Stage. The Contractor shall provide at least one (1) FTE to support the Configuration and Customization work under this Contract on an annual basis during the Ongoing Operation and Enhancement Contract Stage. This support shall include Testing and Validation, Business Analysis, Technical Writing, System Documentation and Project Management required to support the Configuration and Customization hours described herein. The hours of work associated with the FTEs that the Contractor shall provide are shown in the following table, but the Contractor may adjust the hours between types of FTEs as necessary.

4.2.1. Included Enhancement Hours Table

Enhancement Position	**Included Hours each year**
Customization Staff	2,080
Configuration Staff	4,160
Testing and Validation Staff	1,000
Business Analyst Staff	1,000
Technical Writing and System Documentation Staff	500
Project Management Staff	500
Total Annual Hours	**9,240**

4.3. The Department may add additional FTE or hours, at the rates shown in Exhibit E, Section 1.1.3.1, Enhancement Project Rate Table, through the use of an Option Letter.

4.4. The Contractor shall report monthly upon the status of hours expended on a per project basis and those left for that year of the PBMS Ongoing Operations and Enhancement Contract Stage as described in the Communications Plan. On a quarterly basis, the Contractor shall prepare a report for the Department's approval describing how it shall meet the total annual Enhancement hours. With the Department's approval, the Contractor shall be allowed to roll over up to a maximum of 500 hours to the next year of the PBMS Ongoing Operations and Enhancement Contract Stage year.

4.5. Enhancement Pool hours shall be prorated on a monthly basis during the final Contract Year, without affecting the Monthly Payments as described in Exhibit E.

5. DELIVERABLE SUBMISSION AND ACCEPTANCE REQUIREMENTS

5.1. Deliverables

5.1.1. Deliverables shall include all items that result in a written document, implementation of the PBMS and all items specified in Exhibit C.

5.1.2. For each deliverable the Contractor shall comply with all of the following submission and acceptance requirements:

5.1.2.1. A Deliverable Expectation Document shall be developed by the Contractor ahead of actual deliverables. The Deliverable Expectation Document shall contain a template design, table of contents, acceptance criteria, requirements and preparation and review schedule for the deliverable.

5.1.2.2. The Contractor shall submit each deliverable to the Department for review. The Department will review each deliverable and may approve the deliverable or may direct the Contractor to make changes to the deliverable consistent with the Deliverable Expectation Document.

5.1.2.2.1. Changes directed by the Department may include, but are not limited to, changes to any information or portion of the deliverable, the addition of information to the deliverable, the removal of information from the deliverable or rewriting any portion of the deliverable.

5.1.2.2.2. After the development and the Contractor's quality review of a draft or new deliverable, the deliverable is ready for the Department to review. Based on the Contractor's standard deliverable management process, the first draft review allows ten (10) Business Days for the Department to review and provide comments or approve the deliverable. After the first draft review is complete and no comments are received by the end of the ten (10) Business Days, the Contractor will request signatory approval from the Department. The Department and the Contractor may mutually agree upon an extension of the ten- (10)-Business Day review period for large deliverables, as specified in the Deliverable Expectation Document.

5.1.2.2.3. If the Department returns comments or rejects the deliverable, the Contractor shall complete the Department's requested changes to the document and a second review process begins once the Contractor has completed the Department's requested changes and delivered the changed deliverable to the Department. The second review process allows five (5) Business Days for the

Department to review and provide comments on the changes (without the addition of new modification requests) or approve the document. After the second review is complete and no comments are received by the end of the five (5) Business Days, the Contractor will request signatory approval from the Department. The Department and the Contractor may mutually agree upon an extension of the five- (5)-Business Day review period for large deliverables, as specified in the Deliverable Expectation Document.

5.1.2.2.4. If the Department does not approve the document during the second five- (5)-day review process, then the Contractor shall complete the Department's requested changes. The review process allows two (2) Business Days for the Department to review and provide comments on the changes (without the addition of new modification requests) or approve the document once the Contractor has completed the Department's requested changes and delivered the changed deliverable to the Department.

5.1.2.2.5. For the purposes of Quarterly Milestones, the following shall apply:

5.1.2.2.5.1. After the Department's first ten (10) Business Day review period, the Contractor shall complete all changes within ten (10) Business Days.

5.1.2.2.5.2. After the Department's five (5) Business Day review period, the Contractor shall complete all changes within five (5) Business Days

5.1.2.2.5.3. The Contractor shall complete all requested changes following the Department's two (2) Business Day review period in two (2) Business Days.

5.1.2.2.5.4. The Department and the Contractor may mutually agree upon an extension of the Department review and Contractor change periods for large deliverables.

5.1.3. The Contractor shall not make any electronic media or web site available to the public prior to the Department's acceptance of that electronic media or web site.

5.1.4. Each section in a requirement in Exhibit C headed with the term "Deliverable:" is intended to highlight the deliverable in that requirement, but is not intended to expand or limit the deliverable in the requirement in any way.

5.1.5. The Department and the Contractor may change the name of the specified Deliverables and the names of any documents in Exhibit C as they may mutually agree, by using the Transmittal process.

6. TRANSMITTALS

6.1. The Department will use a Transmittal process to provide the Contractor with official direction within the scope of the Contract. The Contractor shall comply with all direction contained within a completed Transmittal. For a Transmittal to be considered complete, it must include, at a minimum, all of the following:

6.1.1. The date the Transmittal will be effective.

6.1.2. Direction to the Contractor regarding performance under the Contract.

6.1.3. A due date or timeline by which the Contractor shall comply with the direction contained in the Transmittal. If the Contractor cannot meet the due date or timeline contained in the Transmittal, it shall work with the Department to determine a mutually agreeable due date or timeline.

6.1.4. The signature of the Department employee who has been designated to sign Transmittals.

6.1.4.1. The Department will provide the Contractor with the name of the person it has designated to sign Transmittals on behalf of the Department, who will be the Department's primary designee. The Department will also provide the Contractor with a list of backups who may sign a Transmittal on behalf of the Department if the primary designee is unavailable. The Department may change any of its designees from time to time by providing notice to the Contractor through a Transmittal.

6.1.4.2. The Department may use an electronic signature to sign any Transmittal.

6.2. The Department may deliver a completed Transmittal to the Contractor through a communication or file sharing system, such as Microsoft SharePoint, that the Parties have designated for such purpose.

6.2.1. In the event that the designated communication or file sharing system is unavailable, the Department may deliver a Transmittal through an email or as a hard-copy document.

6.3. If the Contractor receives conflicting Transmittals, the Contractor shall contact the Department's primary designee, or backup designees if the primary designee is unavailable, to obtain direction. If the Department does not provide direction otherwise, then the Transmittal with the latest effective date shall control.

6.4. In the event that the Contractor receives direction from the Department outside of the Transmittal process, it shall contact the Department's primary designee, or backup designees if the primary designee is unavailable, and have the Department confirm that direction through a Transmittal prior to complying with that direction.

6.5. Transmittals may not be used in place of an amendment, and may not, under any circumstances be used to modify the term of the Contract or any compensation under the Contract. Transmittals are not intended to be the sole means of communication between the Department and the Contractor, and the Department may provide day-to-day communication to the Contractor without using a Transmittal.

6.5.1. In the event that any item or component described in any Exhibit of this Contract is included in a specific plan or deliverable, the parties may agree to include that item or component in any other plan or deliverable as appropriate. In this event, the Contractor shall request approval from the Department to change the plans or deliverables in which the item is included prior to making the change. The Department may approve this change through the use of a Transmittal.

6.6. The Contractor shall retain all Transmittals for reference and shall provide copies of any received Transmittals upon request by the Department.

6.7. Completion of any Transmittal that would require the use of the Change Management Process shall be completed through the Change Management Process instead of through a Transmittal.

7. QUARTERLY MILESTONES

7.1. The Contractor shall include all Quarterly Milestones in its Project Management Plan as well as the calendar quarter in which the Contractor is required to meet that Quarterly Milestone. To allow for project initiation and start-up activities, the first quarter of the Contract will not have a Quarterly Milestone.

7.2. The Contractor shall complete all Quarterly Milestones contained in the most recently approved Project Management Plan in the calendar quarter listed for that Quarterly Milestone. The Parties may change any future Quarterly Milestone by modifying the Project Management Plan. The Parties may not modify any Quarterly Milestone after the calendar quarter has begun in which the Contractor was required to meet that Quarterly Milestone.

8. FORECASTED CLAIMS/ENCOUNTERS

8.1. The Department has forecasted claims and Encounters for the anticipated term of this Contract. These forecasts are intended to be used by the Parties as informational resources to anticipate growth in claims and Encounters and as a baseline for the Contractor to request a Contract change as described in Section 7.G, Option to Increase or Decrease Statewide Quantity of Service, of this Contract. The annual forecasted claims/Encounters are shown in the following table:

8.1.1. Forecasted Claims/Encounters Table

SFY	Annual Claim/Encounter Volume
SFY 2016-17	57,000,000
SFY 2017-18	58,000,000
SFY 2018-19	58,000,000
SFY 2019-20	58,000,000
SFY 2020-21	58,000,000
SFY 2021-22	59,000,000
SFY 2022-23	59,000,000
SFY 2023-24	59,000,000

8.1.2. This table includes paid and denied Fee-for-Service (FFS) medical, dental and pharmacy claims, capitations, and encounters as processed by the PBMS or MMIS contractor and available to the Department to query and report from the BIDM. The volume does not include claims that are rejected by the PBMS or MMIS contractor for data that is missing or invalid or out of compliance.

8.1.3. The Department will provide the prior State Fiscal Year's Annual Claim/Encounter Volume to the Contractor in the third quarter of each calendar year. Upon request from the Contractor, the Department will provide any support materials on how the data was calculated.

9. ADMINISTRATIVE REPORTING

9.1. The Contractor shall provide the administrative reporting in this section in accordance with the procedures and in such form as prescribed by the State and as described in **Exhibit C**, Requirements and the Communication Management Plan.

9.2. The administrative reporting shall include, at a minimum, all of the following for the period that the report covers:

9.2.1. For Key Personnel described in Exhibit C and Contract Personnel as described in Exhibit A, section 4, include all of the following:

9.2.1.1. Number of separated employees during the period.

9.2.1.2. A listing of the position name, separated employee name and separated employee title for each position opened by each separations.

9.2.1.3. Number of new hires during the period.

9.2.1.4. A listing of the position name, new employee name and new employee title for each position filled during the period.

9.2.1.5. Number of vacant positions during the period.

9.2.1.6. A listing of the position name and the total period of time the position was vacant for each vacant position.

9.2.2. For vacancies in the Contractor's Call Center, the Contractor shall include the following:

9.2.2.1. Information on the number of vacant positions, the position name of each vacant position and the total period of time each position was vacant.

9.2.3. The Contractor may include the information regarding Key Personnel, Contract Personnel and Call Center vacancies described in this section in a Monthly Account Management Report Card.

9.3. The Department and the Contractor may agree to modify the content of the administrative reporting under this section through the use of a transmittal and a modification to the Communication Management Plan.

Contract Routing Number 20160000000000002089

EXHIBIT B, SAMPLE OPTION LETTER

Date:	Original Contract Routing # CMS #	Option Letter #	Contract Routing #

1) OPTIONS: Choose all applicable options listed in §1 and in §2 and delete the rest.

a. Option to renew only *(for an additional term)*

b. Change in the amount of goods within current term

c. Change in amount of goods in conjunction with renewal for additional term

d. Level of service change within current term

e. Level of service change in conjunction with renewal for additional term

2) Option to initiate next phase of a contract

REQUIRED PROVISIONS. All Option Letters shall contain the appropriate provisions set forth below:

a. For use with Options 1(a-e): In accordance with Section(s) of the Original Contract between the State of Colorado, Department of Health Care Policy and Financing **,** and Contractor's Name, the State hereby exercises its option for an additional term beginning Insert start date and ending on Insert ending date at a cost/price specified in Section , AND/OR an increase/decrease in the amount of goods/services at the same rate(s) as specified in Identify the Section, Schedule, Attachment, Exhibit etc.

b. For use with Option 1(f), please use the following: In accordance with Section(s) of the Original Contract between the State of Colorado, Department of Health Care Policy and Financing **,** and Contractor's Name, the State hereby exercises its option to initiate Phase indicate which Phase: 2, 3, 4, etc for the term beginning Insert start date and ending on Insert ending date at the cost/price specified in Section .

c. For use with all Options 1(a-f): The amount of the current Fiscal Year contract value is increased/decreased by $ amount of change to a new contract value of Insert New $ Amt to as consideration for services/goods ordered under the contract for the current Fiscal Year indicate Fiscal Year. The first sentence in Section is hereby modified accordingly. The total contract value including all previous amendments, option letters, etc. is Insert New $ Amt.

3) Effective Date. The effective date of this Option Letter is upon approval of the State Controller or , whichever is later.

STATE OF COLORADO
John W. Hickenlooper, GOVERNOR
Department of Health Care Policy and Financing

By: Insert Name & Title of Person Signing for Agency or IHE
Date: _____

ALL CONTRACTS REQUIRE APPROVAL BY THE STATE CONTROLLER

CRS §24-30-202 requires the State Controller to approve all State Contracts. This Contract is not valid until signed and dated below by the State Controller or delegate. Contractor is not authorized to begin performance until such time. If Contractor begins performing prior thereto, the State of Colorado is not obligated to pay Contractor for such performance or for any goods and/or services provided hereunder.

STATE CONTROLLER
Robert Jaros, CPA, MBA, JD

By: _____
Insert Name of Agency or IHE Delegate-Please delete if contract will be routed to OSC for approval
Date: _____

EXHIBIT C, REQUIREMENTS

1. PROJECT GOALS

1.1. Reference #2004: Provide the flexibility to create and modify Pharmacy Benefit Plans within the Pharmacy Benefits Management System (PBMS) such that the services, services limitations, prior authorizations, provider rates, and client cost sharing amounts within a Pharmacy Benefit Plan are easily Configurable through a rule-driven design.

1.1.1. Contractor Approach: The Contractor shall provide a PBMS, a claims adjudication/POS system which is highly configurable, rules and parameter based and table driven, in order to allow complex plan benefit changes to be accomplished by non-technical plan administrators including services, services limitations, prior authorizations, provider rates, and client cost sharing amounts.

1.1.2. Requirement Stage: All Contract Stages

2. CONTRACTOR RELATIONSHIP EXPECTATIONS

2.1. Reference #2005: The Contractor shall be solely responsible for integration of all Work to be performed under the PBMS (and its associated systems) component of the Colorado Medicaid Management Information Technology project, regardless of whether Subcontractors are used. The Contractor shall be responsible for working cooperatively with the prime contractor for the MMIS and the BIDM Contractor.

2.1.1. Contractor Approach: The Contractor anticipates performing all PBMS requirements described in this Contract without the need to hire subcontractors. In the event that the use of (a) subcontractor(s) becomes necessary, the Contractor shall provide the Department with thirty (30) days' notice and shall solely be responsible for all integration work and shall serve as the single point of contact. In addition, the Contractor shall work closely and collaboratively with the prime contractor(s) for the MMIS and BIDM projects.

2.1.2. Requirement Stage: All Contract Stages

3. COMMIT PROJECT PHASES, ALL PHASES

3.1. Reference #2006: Design, develop, test, and implement changes and Enhancements, per the Configuration Management Plan, that may be selected by the Department through the Configuration Management Process for implementation during the duration of the Contract.

3.1.1. Contractor Approach: The Configuration Management plan shall be a component of the larger Project Management Plan, and shall describe the Contractor's approach to design, development, testing and implementation of changes to its systems.

3.1.1.1. The Contractor shall work with the Department on an orderly approach to deliver these changes. Each identified configuration shall follow the Contractor's SDLC.

3.1.1.2. The Contractor shall work with the Department on which of the 12 phases of the contract each configuration change shall be delivered.

3.1.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

3.2. Reference #2007: Provide a report to the Department regarding all PBMS changes that have been implemented in the previous month as well as a projection of Change Requests that will be implemented in the upcoming months.

3.2.1. Contractor Approach: The Contractor shall provide its Change Management approach covering the 12 phases of the contract, including the DDI and Operational phases. The approach shall cover providing the PBMS change report detailing changes made in the previous month. Furthermore, the Contractor shall provide a projection of Change Requests planned and when the Contractor expects these changes to be implemented.

3.2.1.1. Planned changes shall not include benefit plan adjustments or other configuration changes, and shall be reserved for Change Requests requiring changes to the Contractor's systems. System changes shall be defined as underlying code changes to the Contractor's core applications or to those system components that maintain system interoperability, such as data interfaces.

3.2.1.2. The presentation of the PBMS change report and projection of future Change Requests, also known as a Release Plan, shall be detailed in the agreed upon Communication Plan established during DDI.

3.2.2. Deliverable: Monthly PBMS Change Report

3.2.3. Deliverable Stage: PBMS Ongoing Operations and Enhancement Contract Stage

3.3. Reference #2008: Provide the ability to revert to the previous Configurations if the newly implemented change cause an undesirable System impact, within a defined time period in the Change Request.

3.3.1. Contractor Approach: The Contractor shall maintain the ability to revert to previous configurations of its FirstRx POS and eRebate systems based on the Contractor's use of effective dating logic and logical deletion.

3.3.1.1. FirstRx, shall be an on-line, real-time, table-driven system that allows authorized users to define and update business rules in real-time. All changes to business rules shall include an effective date and termination date. Every record that contains an effective date shall be assigned its own sequence number by the database. When an existing record is modified, a new record shall be created from the contents of the original record. This new record shall then be assigned another sequence number with full audit history. The effective date and the sequence number shall tell the system which record should be used in the adjudication process. In the event an undesirable system impact is discovered, these features shall provide the ability to revert to previous Configurations.

3.3.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

3.4. Reference #2009: Document results of lessons learned for each Enhancement, and incorporate that information into the Change Management Plan to reduce the occurrence of defects in future artifacts and processes (continuous improvement).

3.4.1. Contractor Approach: Through a progressive elaborative effort, the Contractor shall review and update its Change Management Plan to effectively leverage lessons learned from prior Enhancement implementations. To ensure success, the Contractor's project team shall develop a living lessons learned document during DDI and shall carry the

lessons learned document through all 12 phases of the implementation and in the PBMS Ongoing Operations and Enhancement Contract Stage.

3.4.2. Requirement Stage: All Contract Stages

3.5. Reference #2010: Implement, maintain and monitor an internal quality control process to ensure that all Deliverables, documents, and calculations are complete, accurate, easy to understand, and of high quality. Include a process to record and address corrective and preventive actions.

3.5.1. Contractor Approach: The Contractor shall maintain an internal quality control processes and promote quality standards. This includes, but is not limited to, the following:

3.5.1.1. On a recurring basis, a random statistically valid sample of claims shall be reviewed by the Contractor team to validate claims processing, including establishing that adjudication algorithms are complete, accurate and of high quality.

3.5.1.2. The Contractor shall review all documents and written deliverables prior to submission to the Department or publication, including all documents delivered to the Department as well as documents produced for the public.

3.5.1.3. Contractor shall implement and maintain a process to ensure all rebate calculations and all documents related to the rebate process are accurate and of high quality.

3.5.2. The Contractor shall provide a documented process to record and address corrective and preventative actions to the Department.

3.5.3. Requirement Stage: All Contract Stages

3.6. Reference #2011: As defined in the Communication Management Plan, develop and provide standards and templates for all documentation and communications for review and approval by the Department.

3.6.1. Documentation and communication includes:

3.6.1.1. Weekly Status Reports.

3.6.1.2. Monthly Status Reports.

3.6.1.3. PBMS Generated Reports.

3.6.1.4. Meeting Agendas.

3.6.1.5. Meeting Minutes.

3.6.2. Contractor Approach: The Contractor shall produce a Communication Management Plan during the Initiation Phase of the Implementation Stage. This Communication Management Plan shall set the communications framework for this project and shall serve as a guide for communications throughout the life of the project. The plan shall be updated, as communication needs change.

3.6.2.1. The plan shall identify and define the roles of persons involved in the PBMS Project and shall include a communications table that maps the communication requirements of the project. The Contractor’s Project Manager shall take a proactive role in ensuring effective communications to all stakeholders involved in

the PBMS Project. The Communication Management Plan shall include standards and templates for all documentation and communications for review and approval by the Department.

3.6.2.2. The Communication Management Plan and communication meetings shall include:

3.6.2.2.1. Weekly Status Reports: Developed, maintained and produced by the Contractor's Project Manager.

3.6.2.2.2. Monthly Status Reports: Developed, maintained and produced by the Contractor's Project Manager.

3.6.2.2.3. PBMS Generated Reports: Developed, maintained, and produced by the Contractor's Business Intelligence Group.

3.6.2.2.4. Meeting Agendas: Developed and produced by the Contractor's Project Manager for the Department's review and approval.

3.6.2.2.5. Meeting Minutes: Developed and produced by the Contractor's Project Manager, for the Department's review and approval.

3.6.3. Requirement Stage: PBMS Implementation Contract Stage

3.7. Reference #2012: As reasonable, local key personnel shall attend in person, any meeting with the Department or other Department stakeholders at the location of the meeting, unless the Department gives approval to attend by telephone or video conference. In the event that the Contractor has any personnel attend by telephone or video conference, the Contractor shall be responsible for providing the conference line or virtual meeting place.

3.7.1. Contractor Approach: The Contractor shall provide local key personnel (Pharmacy Services Account Manager, Pharmacy Systems Manager) to attend in person, any meeting with the Department or other Department stakeholders at the location of the meeting, as reasonable. In the event the Department grants approval to attend by telephone or video conference, the Contractor shall provide the conference line or virtual meeting place.

3.7.2. Requirement Stage: All Contract Stages

3.8. Reference #2013: As defined in the Communication Management Plan, maintain complete and detailed records of all meetings, PBMS Development Life Cycle documents, presentations, project artifacts and any other interactions or Deliverables related to the project described in the Contract and make such records available to the Department upon request, throughout the life of the Contract.

3.8.1. Contractor Approach: Throughout the project and during program operations, the Contractor shall maintain a web-based electronic document repository that enables authorized individuals to view and share project and program reference materials in an organized and secured fashion. The electronic document repository shall be the intended destination for the Transmittal Log documenting communication between various project stakeholders and the Department.

3.8.2. Requirement Stage: All Contract Stages

3.9. Reference #2014: Provide and maintain current documentation of, including but not limited to, the PBMS's database schema, data dictionaries, entity-relationship diagrams, complete PBMS architecture and Configuration diagrams, network diagrams (as applicable), and interface standards for the entire PBMS, including those supporting Proprietary Contractor Material; however, this does not include proprietary information related to Commercial-Off-The-Shelf (COTS) products. Provide and maintain all service delivery documentation related to the design of each module/ component and its interaction with other modules/ components as appropriate.

3.9.1. Contractor Approach: The Contractor shall maintain current and prior versions of all documentation required by Department in a shared web-based electronic documentation repository. The shared document repository shall be accessible to authorized department users. During the term of the Contract the required documents shall be created and updated by the Contractor and submitted for approval to the Department. Documentation will exclude proprietary information related to the Contractor's COTS products.

3.9.2. Requirement Stage: All Contract Stages

3.10. Reference #2015: Develop and maintain online, current documentation on all operational and reference processes, including desk level procedures for Contractor's staff, that can be viewed by the Department.

3.10.1. Contractor Approach: The Contractor shall maintain current and prior versions of all documentation required on all operational and reference processes in a shared web-based electronic documentation repository accessible to authorized Department users. During the term of the Contract required documents shall be created and updated by the Contractor and submitted for approval to the Department.

3.10.2. Requirement Stage: All Contract Stages

3.11. Reference #2016: Develop and submit for Department approval a Project Management Plan, as defined in the most current edition of "A Guide to the Project Management Body of Knowledge (PMBOK)". The plan shall define how the Contractor shall manage all aspects of the Contract that affect price, schedule, performance (scope and quality), risk/ issues/ opportunities, and applicable resources.

3.11.1. The plan shall include at a minimum:

3.11.1.1. Approach for executing monitoring and controlling the project.

3.11.1.2. Approach for managing resources and training, communication and reporting, scope, schedule and cost, and changes.

3.11.1.3. Approach to configuration management.

3.11.1.4. Deliverable review and acceptance procedures.

3.11.1.5. Systems Development Life Cycle approach.

3.11.2. Contractor Approach: The Contractor shall develop a Project Management Plan prior to the implementation kick-off meeting and shall review and update the Project Management Plan throughout the 12 phases of the implementation.

3.11.2.1. The Project Management Plan shall contain ancillary management plans describing the Contractor's approach to Change Management, Communication Management, Risk Management, Configuration Management, Release Management, Quality Management and potentially other key areas of knowledge as described in the PMI Project Management Body of Knowledge (PMBOK). The PMI areas of knowledge shall be applied at the discretion of the Contractor's implementation manager in conjunction with the Department.

3.11.2.2. The Contractor shall also develop and validate with the Department a Project Work Breakdown Schedule in Microsoft Project. The Project Work Breakdown Schedule shall detail the Contractor's approach to executing and monitoring the PBMS implementation. The Project Work Breakdown Schedule shall also demonstrate the Contractor's approach to managing resources, communication and reporting, scope, schedule and cost.

3.11.2.3. In collaboration with the Department, the Contractor's implementation team shall develop and finalize a detailed work breakdown structure (WBS) and schedule using a detailed requirements traceability matrix (RTM) that identifies every requirement of the PBMS and Services implementation.

3.11.3. Deliverable: Project Management Plan, Project Work Breakdown Schedule, Work Breakdown Structure, Requirements Traceability Matrix.

3.11.4. Deliverable Stage: PBMS Implementation Stage

4. COMMIT PROJECT PHASES, INITIATION AND PLANNING PHASE

4.1. Reference #2017: Establish a project management structure to manage projects related to PBMS implementation, PBMS maintenance, and ongoing operations throughout the Contract Stages, generate project-related work products and Deliverables, and report project status to the Department team. The project management structure will be responsible for generating key project management tools.

4.1.1. Contractor Approach: The Initiation and Planning Phase shall include the Department's and Contractor's initial project planning and set up activities. This shall include activities to promote project planning, bi-directional knowledge transfer, improving the Contractor's understanding of the Colorado Medical Assistance program via familiarization activities, communication, and team-building activities to develop a collaborative working relationship between the Department and Contractor. The Contractor shall work with the Department to establish key project planning documents and Deliverables, including the Work Breakdown Schedule, Risk Management Plan, Communication Management Plan, Change Management Plan, and Resource Management Plan.

4.1.2. Requirement Stage: PBMS Implementation Contract Stage

4.2. Reference #2018: Build and maintain the Project Work Breakdown Schedule, as defined in the most current edition of the PMBOK, that includes both Contractor and Department tasks. All tasks shall be identified at a detailed level of a rolling ninety (90) calendar day basis, unless otherwise coordinated and agreed to by the Department.

4.2.1. The Contractor shall deliver this Project Work Breakdown Structure to the Department for review and approval.

4.2.2. The Contractor shall work with the Department to make weekly updates to the Project Work Breakdown Schedule.

4.2.3. Contractor Approach: The Contractor shall structure the scheduled project activities to serve as the tool for managing project tasks assigned to both the Contractor and the Department. The overall Project Management Plan and Work Breakdown Structure (WBS) shall include all tasks and deliverables related to integration activities at a detailed level covering a rolling ninety (90) calendar day basis, unless otherwise coordinated and agreed to by the Department. In addition to the WBS, the overall Project Management Plan shall include a list of potential risk factors and will continuously be monitored. The WBS shall serve as the primary tool for navigation through the project phases up to and including implementation. A cross-functional team of project stakeholders consisting of clinical, technical and operational experts shall work in conjunction with the Contractor's implementation project manager to monitor and determine if risk levels are elevating. In the event of elevated integration risk, the Contractor's team shall quickly assemble a mitigation team, comprised of a range of specialists to fully assess the risk, develop a mitigation plan, and execute on the plan to maintain project milestones and keep critical path tasks as defined in the WBS on target for completion without disrupting the program's operation.

4.2.3.1. The Contractor's project management structure shall manage all tasks related to the PBMS implementation, PBMS maintenance, and ongoing operations throughout the Contract phases.

4.2.3.2. The Project Work Breakdown Schedule shall be used to structure when project-related work and deliverables are due, in order for the project tasks to be tracked, controlled, reported, completed, and approved.

4.2.3.3. The project management plan and stage gate review criteria shall be reviewed during the scheduled kick-off meeting. During this phase, the Contractor's Project Manager shall work collaboratively with the Department to obtain a clear understanding of the Department's current strategic and Project objectives and the Contract's requirements and specifications.

4.2.3.4. The Department shall receive a detailed step-by-step plan on the Contractor's approach to perform services, specifically for the technical infrastructure, system engineering, testing plans, and shared services.

4.2.4. Deliverable: Project Work breakdown Schedule

4.2.5. Deliverable Stage: PBMS Implementation Contract Stage

4.3. Reference #2019: Develop a Quality Assurance (QA) Control/ Quality Management Plan by business activity to address the needs and specific opportunities for quality improvement throughout the Contract period.

4.3.1. The QA Control/ Quality Management Plan should reflect the Contractor's experience and resolve toward:

4.3.1.1. Methodology for maintaining quality of the code, workmanship, project schedules, Deliverables, and Subcontractor(s) activities.

4.3.1.2. Quality in systems design, testing, and implementation.

4.3.1.3. Process design and staff training.

4.3.1.4. Performance standards development and measurement.

4.3.1.5. Customer satisfaction measurement and analysis.

4.3.2. Contractor Approach: The Contractor shall develop a Quality Assurance Control/Quality Management Plan by business activity for use throughout the Contract term. This plan shall outline the following fundamental components of quality management:

4.3.2.1. Ongoing process improvement using Define, Measure, Analyze, Improve and Control (DMAIC) principles

4.3.2.2. Project Management using PMBOK principles

4.3.2.3. Requirements Management using Business Analysis Book of Knowledge (BABOK) principles

4.3.2.4. Testing Strategies, plans and results of all code and system performance

4.3.2.5. Release Management

4.3.2.6. Training

4.3.2.7. Audit

4.3.2.8. Performance Management, including customer satisfaction measurement

4.3.2.9. Reporting.

4.3.3. Deliverable: QA Control/ Quality Management Plan

4.3.4. Deliverable Stage: PBMS Implementation Contract Stage.

4.4. Reference #2020: Develop a Communications Management Plan, as defined in the most current edition of the PMBOK, for the services outlined in the Contract.

4.4.1. The Communications Management Plan shall describe, at a minimum:

4.4.1.1. The Contractor's communication model with the Department and other entities.

4.4.1.2. The Contractor's approach to meeting the communication requirements throughout the course of the Contract performance period.

4.4.1.3. Approach to maintaining telephone and email contact with the Department's assigned Division Director and other designated staff on at least a weekly basis throughout the Contract period.

4.4.1.4. During critical implementation, development, and transition phases, approach to maintaining daily contact with the Department's project managers, as appropriate.

4.4.1.5. The Project Stakeholders.

4.4.1.6. The frequency and breadth of communication.

4.4.1.7. Communication methods.

4.4.1.8. The individuals responsible for communication including valid and after-hour contact information.

4.4.1.9. The review and approval process, including a process for facilitating a Department review of each Deliverable outline and draft documents to ensure common understanding of the purpose and content of documentation prior to final delivery.

4.4.1.10. Create Standard PBMS Report Templates.

4.4.1.11. Establish the Quarterly Milestone reporting schedule.

4.4.1.12. Establish the trigger mechanism for initiating the Dispute Process (e.g., formal letter, email, phone contact).

4.4.2. Contractor Approach: The Communication Plan shall be a component of the overall implementation Project Management Plan, and shall include all elements described in this requirement. In conjunction with the Department, the Contractor shall establish a Communication Plan in the Initiation Phase of DDI and continuing through all 12 phases of the PBMS implementation.

4.4.2.1. Leveraging best practices described in the PMI PMBOK, the Contractor shall develop a Communication Plan in conjunction with the Department. At a minimum, the Contractor shall describe its approach to meeting the communication requirements within the PBMS contract. This shall include the Contractor's approach to maintaining daily contact with the Department's project management team, project stakeholders, and the frequency of communication, and the channels to be used for communication.

4.4.2.2. The Contractor shall establish a standard PBMS status report template and the frequency for which status updates shall be provided. Additionally, the Contractor shall provide quarterly milestone reporting in conjunction with its Project Management Plan, and describe the trigger mechanism for communicating any missed milestones or risks, as per the Risk Management Plan, throughout the 12 phases of the PBMS implementation.

4.4.3. Deliverable: Communications Management Plan

4.4.4. Deliverable Stage: PBMS Implementation Contract Stage

4.5. Reference #2021: The Contractor shall develop a Risk Management Plan to ensure that risks are identified, analyzed, mitigated, communicated, and solutions to identified risks are effectively executed.

4.5.1. Contractor Approach: The Risk Management Plan shall be a component of the overall implementation Project Management Plan and shall include all elements described in this requirement. In conjunction with the Department, the Contractor shall establish a Risk Management Plan in the Initiation Phase of DDI.

4.5.1.1. The Risk Management Plan shall describe the Contractor's approach to identifying risk, assigning a risk score, developing a risk mitigation plan, assigning a risk owner and monitoring and reporting on the risks identified. As part of the Risk

Management Plan, the Contractor shall maintain a risk register throughout the 12 phases of the PBMS implementation.

4.5.1.2. In conjunction with the Communication Plan, new risks and updates on current risks being monitored shall be shared with the Department.

4.5.2. Deliverable: Risk Management Plan

4.5.3. Deliverable Stage: PBMS Implementation Contract Stage

4.6. Reference #2022: Provide a Business Continuity and Disaster Recovery Plan.

4.6.1. The Business Continuity and Disaster Recovery Plan shall include:

4.6.1.1. Timely failover and redundancy.

4.6.1.2. Data recovery.

4.6.1.3. Claims/ encounters processing.

4.6.1.4. Short- and long-term continuity operations.

4.6.1.5. Remote access (in accordance with Department standards).

4.6.1.6. An alternate business site if the primary business site becomes unsafe or inoperable.

4.6.1.7. Root cause analysis reporting to the Department for unscheduled downtime.

4.6.1.8. Provide data backup.

4.6.1.9. Schedule and process for testing of the Business Continuity and Disaster Recovery Plan.

4.6.2. The Contractor shall ensure that the Business Continuity and Disaster Recovery Plan complies with the Colorado System Security Plan Template.

4.6.3. Contractor Approach: As defined by HIPAA Security Administrative procedure requirements, the Contractor shall maintain a Disaster Recovery – Business Continuity Contingency Plan (DR-BCCP) for responding to a system emergency.

4.6.3.1. The plan shall include performing back-ups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, communications and outreach during the disaster, and returning to normal operations following the disaster.

4.6.3.2. A full data center recovery plan shall be included that details recovery processes for each system. The plan shall include defined recovery roles and responsibilities, systems backup and recovery procedures, off-site media storage details, detailed hardware and software configurations /specifications, and emergency & critical business contacts information.

4.6.3.3. The Contractor shall maintain up-to-date disaster recovery procedures and plans as the technical infrastructure and asset inventory evolve.

4.6.3.4. The Contractor shall be responsible for maintaining any necessary contracts with third party vendors that support any or all its recovery services.

4.6.3.5. The Contractor shall address the following in its DR-BCCP:

4.6.3.5.1. Timely failover and redundancy.

4.6.3.5.2. Data recovery.

4.6.3.5.3. Claims/ encounters processing.

4.6.3.5.4. Short- and long-term continuity operations.

4.6.3.5.5. Remote access (in accordance with Department standards).

4.6.3.5.6. An alternate business site if the primary business site becomes unsafe or inoperable.

4.6.3.5.7. Root cause analysis reporting to the Department for unscheduled downtime.

4.6.3.5.8. Provide data backup.

4.6.3.5.9. Schedule and process for testing of the Business Continuity and Disaster Recovery Plan.

4.6.4. Deliverable: Business Continuity and Disaster Recovery Plan

4.6.5. Deliverable Stage: PBMS Implementation Contract Stage

5. COMMIT PROJECT PHASES, DISCOVERY AND REQUIREMENTS VALIDATION/ REQUIREMENTS ELICITATION PHASE

5.1. Reference #2023: Develop and submit a Requirements Definition and Validation Plan.

5.1.1. The Requirements Definition and Validation Plan shall include, at minimum:

5.1.1.1. A description of the Contractor's approach to capturing the results and problems of Requirement Review and Validation Sessions.

5.1.1.2. Tools that will be used to record and track requirements and problems.

5.1.1.3. A description of how potential training needs will be recorded during the requirements sessions.

5.1.1.4. Develop and submit a Requirements Review and Validation Session schedule for review by the Department.

5.1.1.5. Develop and distribute Requirements Review and Validation Session agendas prior to each session.

5.1.1.6. Facilitate requirements review and validation sessions to validate Contract requirements (as listed in this Exhibit C, Requirements) with the Department.

5.1.1.7. Conduct interviews with Department staff to validate, clarify, update, and finalize requirements.

5.1.2. Contractor Approach: The Contractor shall develop and submit a Requirements Definition and Validation Plan that includes all of the required elements:

5.1.2.1. The Contractor's approach shall include a standard process to facilitate, document, and version requirements throughout the implementation and operations phases of the project.

5.1.2.2. The Contractor shall create a Requirements and Performance Standards Traceability Matrix to track and record all Contract requirements, associated functional requirements, and test results.

5.1.2.3. The Contractor shall execute requirements review and validation sessions with the Department to clarify, validate and finalize all requirements. Agendas and minutes shall be recorded prior to and after sessions. The Department staff shall be interviewed individually as well to validate, clarify, update, and finalize requirements.

5.1.3. Deliverable: Requirements Definition and Validation Plan

5.1.4. Deliverable Stage: PBMS Implementation Contract Stage

5.2. Reference #2024: Develop and submit to the Department a draft Requirements Specifications Document (RSD) for Contractor-proposed PBMS components, modules and functional areas.

5.2.1. At minimum, the RSD shall include:

5.2.1.1. An overview of PBMS architecture and how components are integrated.

5.2.1.2. Detailed Requirements Specification Template.

5.2.1.3. Identification of changes to existing requirements.

5.2.1.4. Clarifying information associated with requirements, as needed.

5.2.1.5. Identification of new requirements.

5.2.1.6. Explanation of how requirements will be met.

5.2.1.7. Identification of the entity responsible for meeting the requirement.

5.2.1.8. Description of the hardware/ software Configuration that will be used to meet the requirement.

5.2.1.9. A logical data model that identifies all entities, relationships, attributes, and access paths.

5.2.2. Contractor Approach: The Contractor shall develop and submit a document or series of documents to create a Requirements Specifications Document (RSD) for Contractor-proposed PBMS components, modules and functional areas.

5.2.3. Deliverable: Draft RSD

5.2.4. Deliverable Stage: PBMS Implementation Contract Stage

5.3. Reference #2025: Compile the final RSD that incorporates the Department’s review findings to reflect all requirements that need to be met as defined in the facilitated Requirement Review and Validation Sessions. Detailed requirement specifications may be delivered incrementally, as they are developed for each functional component or module.

5.3.1. Contractor Approach: The Contractor shall compile the final Requirements Specification Document (RSD) that incorporates the Department's review findings resulting from the Requirement Review and Validation Sessions.

5.3.2. Deliverable: Final RSD

5.3.3. Deliverable Stage: PBMS Implementation Contract Stage

5.4. Reference #2026: Develop and maintain a Business Rules Traceability Matrix to ensure that the PBMS appropriately applies business rules in compliance with the Pharmacy Benefit Plan requirements.

5.4.1. Contractor Approach: The Contractor shall develop and maintain a Requirements Analysis Document (RAD) which shall include a Business Rules Traceability Matrix. The RAD shall document the functional business rules that are in place for the benefit plans managed under this Contract after they have been discussed, validated, and confirmed with the State. The RAD shall serve as a basis for developing test cases to validate the proper functioning of the rules prior to their deployment into production.

5.4.2. Deliverable: Business Rules Traceability Matrix

5.4.3. Deliverable Stage: PBMS Implementation Contract Stage

5.5. Reference #2027: Develop and maintain a Requirements Traceability Matrix (RTM) to ensure that detailed requirements comply with Contract requirements.

5.5.1. Contractor Approach: The Contractor's RAD shall map back to the RTM that identifies every Department requirement. In addition to the detailed business requirements, rules and data needs, the Contractor's documentation shall capture project objectives, scope, dependencies, assumptions, risks and constraints. The Contractor shall submit documentation to the Department for review and approval.

5.5.2. Deliverable: Requirements Traceability Matrix

5.5.3. Deliverable Stage PBMS Implementation Contract Stage

6. COMMIT PROJECT PHASES, DESIGN AND DEFINITION PHASE

6.1. Reference #2028: Develop and submit a Detailed System Design Plan.

6.1.1. The Detailed System Design Plan shall include, at minimum:

6.1.1.1. Approach to tracking results and problems from Detailed PBMS Design Sessions.

6.1.1.2. Tools to be used to manage session results and problems.

6.1.1.3. Approach to capturing and tracking potential training considerations identified during design sessions.

6.1.1.4. The format of the proposed Design Specification Document (DSD) Deliverable.

6.1.2. Contractor Approach: The Contractor shall develop and submit a Detailed System Design (DSD) plan that includes details about how the systems and services will be implemented to support the Department. The Contractor shall include technical diagrams that illustrate the solution components, as well as present a client-server computing platform with the inventory of hardware, software, networking, and data parts as well as databases. The plan shall include the approved requirements gathering process, how the items shall be built and configured. The plan shall also include testing and approval by the Department prior to being deployed into production. The process shall begin with the Contractor's subject matter experts (SMEs) updating

template DSD's based on their understanding of the requirements as they were communicated during proposal phase. The implementation project manager shall then identify SMEs from the program and schedule meetings to collaborate with the Contractor's SMEs to validate each requirement in the customized template and discuss if there are any additional requirements. These meetings shall be facilitated by the implementation project manager who shall document meeting minutes with action items in Microsoft Word documents and post them to the shared document repository. Possible action items shall include, but not be limited to, additional information gathered on both sides and other documents that require updating or training material updates necessitated by decisions made. The exit criteria for this set of tasks shall be Department sign-off of the collaboratively created DSD.

6.1.2.1. If the development and testing processes subsequently identifies a need for additional changes, the Contractor shall evaluate the impact of each change, submit it for project management or Steering Committee approval, and update the change in new versions of the Business Requirements, Functional Requirements, system configuration document, and testing plans (sign offs).

6.1.3. Deliverable: Detailed System Design Plan

6.1.4. Deliverable Stage: PBMS Implementation Contract Stage

6.2. Reference #2029: Develop and submit a Detailed System Design Session schedule for review by the Department.

6.2.1. Contractor Approach: The DDI Project Manager shall coordinate with the various SMEs to customize Contractor's standard templates and to schedule design sessions for review with the appropriate SMEs from the program. Attention shall be given to the amount of time it usually takes to address various design areas and the appropriate number of meetings shall be scheduled for each. The implementation project manager shall then create agendas based on the items that must be collaboratively reviewed from each customized template and distribute them to all invitees. All meetings shall be scheduled with respect to the time constraints of the SMEs from the program. All artifacts shall be posted on the shared document repository.

6.2.2. Deliverable: Detailed System Design Session Schedule

6.2.3. Deliverable Stage: PBMS Implementation Contract Stage

6.3. Reference #2030: Perform prototyping when appropriate to enable Department staff to review and accept windows, screens, reports or other layouts designs.

6.3.1. Contractor Approach: Prototyping may be desired when components of the PBMS User Interface are enhanced or changed through the DDI and Operational phases of the project. Upon request from the Department, the Contractor shall provide User Interface mockups to serve as a prototype view of the system enhancement or change and these mockups will be isolated from the production/operational system. The prototype view of the system component shall be able to be reviewed by the Department and acceptance will allow for the Contractor to move through the next phases of the SDLC. Any desired change to the prototype by the Department shall result in modifying the change or enhancement requirements before iterating through and into the prototype stage for Department approval. Once prototypes are deemed acceptable to the

Department, the change shall be introduced into the operational development environments for design, regression testing, implementation and promotions to production environments following strict adherence to the SDLC.

6.3.2. Requirement Stage: PBMS Implementation Contract Stage

6.4. Reference #2031: Develop and provide to the Department for approval an Environment Architecture and Implementation Plan.

6.4.1. Contractor Approach: An Environment Architecture and Implementation Plan shall be delivered during the Design and Definition Phase that shall serve to identify each architectural system design, purpose, and expected delivery date within the System Development Life Cycle (SDLC). This plan shall include system architecture drawings and crosswalk tables to serve as a quick references to the specific servers, databases, and user interface pages to help testers, plan developers, and other technical staff to attach to the appropriate systems when performing tests, plan creations, or system configuration adjustments.

6.4.2. Deliverable: Environment Architecture and Implementation Plan

6.4.3. Deliverable Stage: PBMS Implementation Contract Stage

6.5. Reference #2032: Develop and provide to the Department for approval a Physical and System Security Plan.

6.5.1. Contractor Approach: The Contractor shall provide a Physical and System Security Plan that is based on International System Security Certification Consortium (ISC2) — the international standard for IT security — and the National Institute of Standards and Technology (NIST). The plan shall include all technical, physical, and administrative safeguards to enhance physical security, personnel security, and information systems security. The plan shall demonstrate the Contractor's compliance with the HIPAA Standards for Privacy, Electronic Transactions and Security.

6.5.1.1. The Physical and System Security Plan shall provide a basis for governance of the privacy and security of the project components provided under the pharmacy program for Colorado. The plan shall outline perimeter protection, segregated operations, business, and administrative architectures, and any extra protective measures necessary for Internet facing systems. This includes ensuring the appropriate placement of firewalls, intrusion detection services, securing and monitoring the network infrastructure, as well as other physical and technical security measures, to ensure continued compliance with the expected service levels required under the Contract.

6.5.2. Deliverable: Physical and System Security Plan

6.5.3. Deliverable Stage: PBMS Implementation Contract Stage

6.6. Reference #2033: Prepare and submit the Detailed PBMS Design Session meeting notes and include the decisions, justification for changes (including new, modified, or deleted requirements), outstanding problems requiring follow-up, and impacts to future detailed design sessions.

6.6.1. Contractor Approach: The Contractor shall work with the Department to gather requirements through design session meetings. The Contractor shall draft a design document that is based on the Contractor's understanding of the requirements as presented in the RAD and that shall be the baseline to drive the agenda of the work sessions. The Contractor shall facilitate design session meetings where a baseline document is collaboratively completed, is acceptable to both Contractor and the Department and receives all necessary sign offs. The detailed PBMS Design Session meeting notes shall include decisions, justification for changes, outstanding problems requiring follow up, and impacts to future detailed design sessions. The Contractor shall post the PBMS Design Session meeting notes, as well as the revisions of the design documents themselves, to the shared document repository, as well as providing them to the Department during the Design and Definition Phase.

6.6.2. Deliverable: Detailed PBMS Design Session Meeting Notes

6.6.3. Deliverable Stage: PBMS Implementation Contract Stage

6.7. Reference #2034: Submit a draft DSD that incorporates comments submitted by the Department.

6.7.1. Contractor Approach: The Contractor shall work with the Department to gather requirements through design session meetings. The Contractor shall draft a Design Specification Document (DSD) that is based on an understanding of the requirements as they were presented in the RAD and that document shall be the baseline to drive the agenda of the work sessions. The DSD shall also include a System Documentation Template including hardware and software descriptions of the services and infrastructural components. The Contractor shall facilitate design session meetings where the baseline document is collaboratively completed, is acceptable to both the Contractor and the Department and receives all necessary sign offs. The notes from these meetings, as well as the revisions of the design documents themselves, shall be posted to the shared document repository and provided to the Department during the Design and Definition Phase.

6.7.2. Deliverable: Draft DSD

6.7.3. Deliverable Stage: PBMS Implementation Contract Stage

7. COMMIT PROJECT PHASES, DEVELOPMENT PHASE

7.1. Reference #2035: Develop a final DSD based on the facilitated design sessions. Detailed design specifications may be delivered incrementally, as they are developed for each functional component or module, with final approval when all are approved. The DSD shall also include a System Documentation Template. Examples of information to be included in the System documentation are hardware and software, descriptions of the services and infrastructural components, and other necessary System information.

7.1.1. Contractor Approach: The Contractor shall work with the Department to gather requirements through design session meetings. The Contractor shall draft a DSD that is based on an understanding of the requirements as they were presented in the RAD and that document shall be the baseline to drive the agenda of the work sessions. The DSD shall also include a System Documentation Template including hardware and software descriptions of the services and infrastructural components. The Contractor

shall facilitate design session meetings where the baseline document is collaboratively completed, is acceptable to both the Contractor and the Department and receives all necessary sign offs. The notes from these meetings, as well as the revisions of the design documents themselves, shall be posted to the shared document repository and provided to the Department during the Design and Definition Phase

7.1.2. Deliverable: Final DSD

7.1.3. Deliverable Stage: PBMS Implementation Contract Stage

7.2. Reference #2036: Update and maintain the RTM with results from Detailed PBMS Design Sessions.

7.2.1. Contractor Approach: The Contractor shall update and maintain the RTM with results from Detailed System Design Sessions.

7.2.2. Deliverable: Updated RTM

7.2.3. Deliverable Stage: PBMS Implementation Contract Stage

7.3. Reference #2037: Develop and submit to the Department a Unit Test Checklist Template and Unit Test Plan that describes the Contractor's approach, methodology and schedule for unit testing of the PBMS.

7.3.1. Contractor Approach: The Contractor shall develop and submit to the Department a Unit Test Checklist Template and Unit Test Plan, for any change that requires the modification of source code that reflects the Contractor's process for unit testing. The Contractor's approach shall be tailored to the functional component being tested.

7.3.2. Deliverable: Unit Test Checklist Template and Unit Test Plan

7.3.3. Deliverable Stage: PBMS Implementation Contract Stage

7.4. Reference #2038: Conduct unit testing and submit results via Unit Test Checklists attesting that each component and module has been thoroughly unit-tested, meets the checklist criteria, and is therefore ready for the PBMS test.

7.4.1. Contractor Approach: The Contractor shall conduct unit testing and submit results via Unit Test Checklists. The checklists shall be tailored to the component being tested, and shall include completed checklists, and final attestation that the system(s) are ready for the PBMS test.

7.4.2. Requirement Stage: PBMS Implementation Contract Stage

7.5. Reference #2039: Provide weekly updates and performance metrics on unit testing and development progress to the Department as part of the weekly status reports.

7.5.1. Contractor Approach: The Contractor shall provide weekly updates and performance metrics on unit testing and development process to the Department as part of the weekly status reports. The Contractor shall use a format for the status reports as approved by the Department.

7.5.2. Deliverable: Weekly Status Report

7.5.3. Deliverable Stage: PBMS Implementation Contract Stage

7.6. Reference #2040: Conduct development walkthroughs as appropriate to demonstrate to the Department that all PBMS functions have been completely and accurately developed and unit-tested and record problems using the project control and problem reporting system prescribed by the Department.

7.6.1. Contractor Approach: The Contractor shall conduct development walkthroughs at various stages of the development cycle to demonstrate that all PBMS functions have been completely developed and unit tested. The Contractor shall record all problems using the project control and problem reporting system prescribed by the Department.

7.6.2. Deliverable: Development Walkthroughs

7.6.3. Deliverable Stage: PBMS Implementation Contract Stage

8. COMMIT PROJECT PHASES, DATA CONVERSION PHASE

8.1. Reference #2041: Takeover existing data and information storage from incumbent contractor. Store and manage specified historical data, including the current drug rebate system and the Legacy System, covering a specified time.

8.1.1. Contractor Approach: The Contractor shall be responsible for the timely and accurate data conversion of historic claims and prior authorizations necessary to adjudicate claims.

The Contractor shall be responsible for the timely and accurate data conversion process for data in the Legacy System, including drug rebate data as specified in the Data Conversion Plan.

8.1.2. Requirement Stage: PBMS Implementation Contract Stage

8.2. Reference #2042: Develop and submit a phased Data Conversion Plan.

8.2.1. The Data Conversion Plan shall provide detailed requirements including, at a minimum:

8.2.1.1. Discovery and Legacy System and Source data evaluation process.

8.2.1.2. Recommended scope of data conversion based on discovery/ evaluation results.

8.2.1.3. Relevant data sources including the Legacy System.

8.2.1.4. Department participation needs in the data conversion process development and execution.

8.2.1.5. Reporting migration requirements, including functionality validation of third-party tools and/or Legacy System and Source data.

8.2.1.6. Documentation of success and failure metrics.

8.2.1.7. Post data migration cleanup process.

8.2.1.8. Final validation and acceptance procedure.

8.2.1.9. Emergency rollback contingency procedures, if applicable.

8.2.2. Contractor Approach: Contractor shall provide a Data Conversion Plan for an End-to-End Integration Test and a User Acceptance Test (UAT) including all pre-production data conversions as verified and approved by the Department.

8.2.2.1. The Contractor shall receive data, and build a data file of all required data from the source system and load the converted data into the target PBMS system databases. Contractor's data conversion process shall use technologies, such as Informatica, Oracle, SQL Server, and Extract Transform and Load (ETL) methodologies, to create migration programs that shall load data from the source system to the target system while producing report exceptions. Contractor's established conversion process shall produce reports and metrics that list all files loaded, number of records loaded, number of records failed, percentages of failures, running totals, dates, run times, etc. The process shall automatically build files of records rejected by reject type to be easily reviewed and, once remediated, easily rerun through the process. The conversion method shall provide exception reports to identify those instances of missing field values, failed editing routines, invalid data formats, etc. Reports shall be delivered to the Department for review. Problems identified as a result of the conversion process shall follow the pre-defined resolution process and shall be reprocessed through an automated update of the data before the conversion into the target system.

8.2.2.2. The Contractor shall perform the conversion following these specific steps:

8.2.2.2.1. Receive or extract data from source system as agreed upon in the requirements sessions.

8.2.2.2.2. Analyze the data and provide counts on conversion data to the Department

8.2.2.2.3. Transform the data from the source to be loaded to the target database.

8.2.2.2.4. Load the data to the target database.

8.2.2.2.5. Validate the loaded data by executing the test scripts pertaining to each conversion.

8.2.2.2.6. Provide data conversion results in the agreed upon format to the Department for review.

8.2.2.2.7. Provide detailed reports of rejected records and work with the Department on data corrections. If the records are rejected due to issues with the Contractor load/transform process, the Contractor shall fix and reload until records are loaded successfully to a point that is accepted by the Department or as agreed upon by Contractor and the Department.

8.2.2.2.8. Repeat steps until all records are loaded to a point that is accepted by the Department.

8.2.3. Deliverable: Data Conversion Plan

8.2.4. Deliverable Stage: PBMS Implementation Contract Stage

8.3. Reference #2043: Acquire the hardware and software needed for a successful data conversion.

8.3.1. Contractor Approach: The Contractor shall procure the hardware and software needed for a successful implementation. The Contractor shall adequately definine all hardware /software design specifications needed during the purchase process. The Contractor shall manage the associated, maintenance and licensing agreements for the purchases

made. The licensing procurements shall accurately reflect the design and usage requirements of the software purchase.

8.3.2. Requirement Stage: PBMS Implementation Contract Stage

8.4. Reference #2044: Implement a fully functioning data migration environment to be used by both the Contractor and Department for current and ongoing migration needs.

8.4.1. Include the following:

8.4.1.1. Relevant tools, utilities, and software.

8.4.1.2. Associated licenses with ownership transferred to the Department.

8.4.1.3. Appropriate access rights for management, operation, and maintenance.

8.4.2. Contractor Approach: The Contractor shall maintain a secure data migration environment that allows the Contractor to perform staging, analysis, and development of ETL processes and verification of output data. The Contractor shall utilize a shared hardware and software environment for the transformation of data, which shall then be placed into the production environment configured for the Department.

8.4.2.1. The Contractor uses various COTS tools and technologies that are part of its existing, shared data center environment. Should the Contractor need to purchase new tools specifically needed for the data migration, the Contractor shall transfer ownership of all licenses for tools purchased specifically for Department's data migration. In addition, appropriate access to the environment shall be granted to Department designated personnel for the purposes of review and analysis of the data as it moves through the process.

8.4.2.2. The Contractor shall provide a data migration environment for each computing environment including those used by the Department’s local agencies and remotely throughout the Department. To support the successful implementation of a data migration environment, the Contractor shall acquire the hardware and software needed for a successful data conversion. The procurement process shall begin on the Effective date and the Contractor shall have the environment installed and ready well in advance of starting conversion activities. Separate servers shall be used for each environment.

8.4.2.3. The Contractor’s approach to data conversion shall address the security and privacy concerns of the technical infrastructure, the computing environments, and all the systems and services authorized users, including exchange data services partners or trading-partners rights to data security, data privacy, and data confidentiality.

8.4.3. Deliverable: Data Migration Environment

8.4.4. Deliverable Stage: PBMS Implementation Contract Stage

8.5. Reference #2045: Revise System and User Documentation as required by the Department.

8.5.1. Contractor Approach: The Contractor shall maintain and revise System and User documentation on an ongoing basis and shall deliver the documentation to all users through format (electronic and/or paper) required by the Department.

8.5.2. Requirement Stage: PBMS Implementation Contract Stage

8.6. Reference #2046: Perform a System test to compare all transferred programs, files, utilities, etc., to determine that the migration was successful.

8.6.1. Contractor Approach: The Contractor shall perform data integrity and conversion integration testing to include record counts, record sampling, and balancing using validation reports comparing the converted data with the source system. The automated methods shall be used to convert and validate converted data.

8.6.1.1. Contractor's established conversion process shall produce reports and metrics that list items such as all files loaded, number of records loaded, number of records failed, percentages of success and failures, running totals, dates and run times. The process shall automatically build files of records rejected by reject type to be easily reviewed and once remediated, easily rerun through the process. The conversion method shall provide exception reports to identify those instances of missing field values, failed editing routines (member not on file, provider not on file), invalid data format, etc. The Contractor shall track problems identified as a result of the conversion process using automated tool by issue type, description, and owner and shall follow the resolution process. The Contractor shall produce pre and post-conversion reports for each interface and table as well as detailed reports of all converted data.

8.6.1.2. The Contractor shall send test result reports to the Department and request that the Department validate the reports, review the rejects, and work with Contractor's analysts in addressing them. The Department shall formally approve the conversion reports prior to the start of operations once it has approved the test results. The formal documentation shall be archived in document management system for future reference.

8.6.2. Deliverable: Completed System Test

8.6.3. Deliverable Stage: PBMS Implementation Contract Stage

9. COMMIT PROJECT PHASES, TESTING PHASE

9.1. Reference #2047: Provide an integrated test environment consistent with the proposed System Development Life Cycle (SDLC) process that allows the Department and the Contractor to monitor the accuracy of the PBMS and test proposed changes to the PBMS by processing test claims/ encounters and other transactions through the PBMS without affecting normal operations. The test environment shall allow for end-to-end testing including transmission of all PBMS data to the BIDM.

9.1.1. The Contractor’s test plan shall contain details of when all environments, including the integrated test environment, will be available.

9.1.2. Contractor Approach: The Contractor shall create and maintain an integrated test environment for testing all functionality required by the Department. This environment shall be independent of the development and production environments, and shall be maintained in both DDI and operations periods. The test environment shall be as close to a mirror of the production environment as reasonable, which includes all data and functions. This environment shall be used for system testing, integration testing, and end-to-end testing, and shall be maintained throughout the life of the Contract.

9.1.3. Deliverable: Integrated Test Environment

9.1.4. Deliverable Stage: PBMS Implementation Contract Stage

9.2. Reference #2048: The test environment shall be sized to be capable of mirroring the production System in its files, databases, processing, and reporting.

9.2.1. Contractor Approach: The test environment shall be sized to be capable of mirroring the production system in its files, databases, processing, and reporting to support application and implementation testing cycles. The test system shall be capable of receiving a full system, database and application refreshes periodically or upon request with no interruption of production operations.

9.2.2. Requirement Stage: PBMS Implementation Contract Stage

9.3. Reference #2049: The Contractor shall verify that Legacy System and PBMS will produce the same results.

9.3.1. Contractor Approach: The Contractor shall perform specific testing (sometimes called parallel testing) to compare the results of transactions processed by the legacy system with results of transactions processed by the PBMS. This testing shall identify any discrepancies between the results of the two processes. Discrepancies shall be researched to understand the root cause of the discrepancy. If the discrepancy is not a result of different requirements, it shall be logged as a defect, fixed, retested, and resolved, with final approval by the Department.

9.3.2. Requirement Stage: PBMS Implementation Contract Stage

9.4. Reference #2050: The test environment(s) shall allow for the processing of mock data from production to populate claims/ encounters with a volume and distribution similar to that of the production system. All system and integration testing shall be performed such that the data is not overwritten by multiple testing initiatives or the refresh. Refreshing data will be scheduled per the Department-approved Change Management Plan and will include the entire PBMS.

9.4.1. Contractor Approach: The Contractor's test environment shall be as close to a mirror of the production environment as reasonable. This shall be a standard approach used by the Contractor to ensure that the test environment most accurately reflects the system performance and behavior of the Department's production environment. The Contractor shall refresh the test environment according to the Department-approved Change Management Plan and in a manner that shall retain previous test data.

9.4.2. Requirement Stage: PBMS Implementation Contract Stage

9.5. Reference #2051: As PBMS improvements or enhancements are implemented, that functionality shall also be deployed to test environments, so that test environments mirror production functionality.

9.5.1. Contractor Approach: The Contractor shall maintain the test environment throughout the term of the Contract. Every change made to the PBMS shall be loaded from a development environment into the testing environment, where it shall be fully tested. Changes shall be bundled into releases approved by the production turnover committee, and shall be scheduled for release to production upon final approval from the

Department. Upon release, the functionality in the production and testing environment shall be the same.

9.5.1.1. In the event that a modification is made to the production environment that was not in the testing environment, the Contractor shall make that modification in the testing environment.

9.5.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

9.6. Reference #2052: Provide the Department with online access to the integrated test environment.

9.6.1. Contractor Approach: The Contractor shall provide the Department with online access to the integrated test environment. This shall allow the Department to perform UAT if desired, and to review test results of the Contractor.

9.6.2. Requirement Stage: All Contract Stages

9.7. Reference #2053: Automate the testing process for changes or Enhancements to the PBMS.

9.7.1. Contractor Approach: The Contractor shall automate the testing for changes or Enhancements to the System. This is especially applicable to regression testing, as well as for retesting during the development cycle.

9.7.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

9.8. Reference #2054: Automate the Defect tracking process for changes or Enhancements to the PBMS.

9.8.1. Contractor Approach: The Contractor shall use an automated Defect tracking tool to track defects both during the DDI phase and the operations period of the project.

9.8.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

9.9. Reference #2055: Develop a System Test Plan that describes the Contractor's approach and commitment to all testing sub-phases required for a system of this magnitude.

9.9.1. The System Test Plan shall include, but is not limited to:

9.9.1.1. System testing process.

9.9.1.2. Integration testing.

9.9.1.3. Data Conversion testing process.

9.9.1.4. Approach to supporting Department during UAT. The UAT process shall provide for authorized System users to exercise the entire System, including the use of converted data, in a separate, controlled environment.

9.9.1.5. Performance/ stress testing.

9.9.1.6. Penetration testing.

9.9.2. The approach to conducting all specified testing for all PBMS programs per Department entrance and exit criterion. Any changes to test cases, including entrance and exit criteria, require written approval by the Department.

9.9.3. Contractor Approach: The Contractor shall develop a System Test Plan that describes the Contractor's approach and commitment to all testing sub-phases required, including but not limited to:

9.9.3.1. System testing process shall be conducted by the Contractor's Quality Assurance team.

9.9.3.2. Integration testing shall be conducted by the Contractor's Quality Assurance team.

9.9.3.3. Data Conversion testing process shall be conducted by the Contractor's Quality Assurance team.

9.9.3.4. Approach to supporting the Department during UAT. The Contractor shall provide authorized System users secure access to the test environment, shall train the Department's UAT testers on both the system and the defect management tool to fully engage the UAT testers. The Contractor's test cases shall be shared if desired, but it is advised that UAT testers create their own, for most robust testing perspective. Since the test environment reflects the production environment, the UAT process shall provide access to the entire system.

9.9.3.5. Performance/ stress testing.

9.9.3.6. Penetration testing.

9.9.3.7. The approach to conducting all specified testing for all System programs per Department entrance and exit criterion. Any changes to test cases, including entrance and exit criteria, require written approval by the Department.

9.9.4. Deliverable: System Test Plan

9.9.5. Deliverable Stage: PBMS Implementation Contract Stage

9.10. Reference #2056: Develop a System Test Plan that describes the Contractor's approach and commitment to all testing sub-phases required for a system of this magnitude.

9.10.1. The System Test Plan shall include, but is not limited to:

9.10.1.1. Roles and responsibilities throughout the Testing Phase.

9.10.1.2. Process for submitting, monitoring, and resolving Defects found during testing and Enhancements and assigning severities/ priorities in accordance to Department standards.

9.10.1.3. Process for applying fixes to the System and regression testing of any fixes.

9.10.1.4. Assurance of parity between technical environments.

9.10.1.5. Description of the proposed system or tool for identifying, prioritizing, tracking, fixing, and re-testing System Defects or Enhancements. This tool may be the same Project Control and Problem Reporting System detailed in Section 7.6.

9.10.1.6. Structured promotion of functionality to subsequent testing levels.

9.10.1.7. Summary of testing tools used throughout the Testing Phase, including the approach to defining test cases that are representative of actual cases.

9.10.1.8. Testing of recovery processes and/ or component outages/ failures.

9.10.1.9. Description of the proposed system or tool for identifying, prioritizing, tracking, fixing, and re-testing System Defects or Enhancements. This tool may be the same Project Control and Problem Reporting System detailed in Section 7.6.

9.10.1.10. Structured promotion of functionality to subsequent testing levels.

9.10.1.11. Summary of testing tools used throughout the Testing Phase, including the approach to defining test cases that are representative of actual cases.

9.10.1.12. Testing of recovery processes and/ or component outages/ failures.

9.10.2. Contractor Approach: The Contractor shall develop a System Test Plan that describes the Contractor's approach and commitment to all testing sub-phases required, including but not limited to:

9.10.2.1. Roles and responsibilities throughout the Testing Phase.

9.10.2.2. Environment specifications

9.10.2.3. Test approach/process

9.10.2.4. Roles and responsibilities of all participants

9.10.2.5. Defect Management process and tool

9.10.2.6. Escalation process

9.10.2.7. Definitions including priority and severity ratings

9.10.2.8. Entrance and Exit criteria

9.10.3. Deliverable: System Test Plan

9.10.4. Deliverable Stage: PBMS Implementation Contract Stage

9.11. Reference #2057: Design, implement, and document detailed test cases for each sub-phase of testing identified in the above requirement. Test cases should include identifications, detailed steps, expected results, actual results (where appropriate), and be traceable to requirements listed in this Contract in the RTM.

9.11.1. Contractor Approach: The Contractor shall design, implement, and document detailed test cases for each sub-phase of testing identified in the System Test Plan. Test cases shall include: identification number, test steps, expected and actual results, associated defect numbers, and Contract and RTM tracking number. This shall be a standard practice for the Contractor.

9.11.2. Deliverable: Detailed Test Cases

9.11.3. Deliverable Stage: PBMS Implementation Contract Stage

9.12. Reference #2058: Submit all Test Results (including Performance/ Stress Testing Results, Final PBMS Test Results, and Penetration Test Results) for each test sub-phase to the Department.

9.12.1. Submitted test results shall include, at minimum:

9.12.1.1. Summary of testing results.

9.12.1.2. Pass/ Failure Rate.

9.12.1.3. Defect IDs and severity level of failed test cases.

9.12.1.4. Proposed resolution for identified defects.

9.12.2. Contractor Approach: The Contractor shall submit all test results , which shall include:

9.12.2.1. Summary of testing results.

9.12.2.2. Pass/ Failure Rate.

9.12.2.3. Defect IDs and severity level of failed test cases.

9.12.2.4. Proposed resolution for identified defects.

9.12.2.5. These results shall be provided by the Contractor to the Department for each of the testing categories, which include the unit test, system test and UAT.

9.12.3. Deliverable: Test Results for all tests performed

9.12.4. Deliverable Stage: PBMS Implementation Contract Stage

9.13. Reference #2059: Perform regression testing for all defects identified as directed by the Department and provide regression testing results.

9.13.1. Contractor Approach: The Contractor shall perform regression testing for all Defects identified by the Contractor or as directed by the Department and provide regression testing results accordingly. Regression testing shall be a standard procedure in the Contractor's overall test approach.

9.13.2. Requirement Stage: All Contract Stages

10. COMMIT PROJECT PHASES, ORGANIZATIONAL READINESS AND TRAINING PHASE

10.1. Reference #2060: Provide regular updates to Department during the Organizational Readiness period.

10.1.1. Contractor Approach: The Contractor’s Implementation Project Manager shall provide regular updates via meetings and written communication on Operational Readiness as outlined in the Communication Management Plan and the operational readiness checklist.

10.1.2. Requirement Stage: PBMS Implementation Contract Stage

10.2. Reference #2061: Provide support to the Department as part of Organizational Readiness, including providing a minimum of one organizational readiness lead and a minimum of two staff members who will be available as required to address questions and concerns.

10.2.1. Contractor Approach: The Contractor shall provide support to the Department as part of Organizational Readiness, including providing a minimum of one organizational readiness lead and a minimum of two staff members who shall be available as required to address questions and concerns. During the Organizational Readiness and Training Phase the Contractor shall provide organizational readiness support in general and training related support.

10.2.2. Requirement Stage: PBMS Implementation Contract Stage

10.3. Reference #2062: Ensure all necessary PBMS access is in place, including passwords, at the time of Organizational Readiness training.

10.3.1. Contractor Approach: Each Department user will complete a user access request based on that user's role and the systems that user needs to access. Once the Contractor receives that request, the Contractor shall create and configure all user access and ensure appropriate access.

10.3.2. Requirement Stage: PBMS Implementation Contract Stage

10.4. Reference #2063: Assist the Department in identifying information to be conveyed to Department staff and providers as part of Organizational Readiness.

10.4.1. Contractor Approach: The Contractor shall schedule a walkthrough with the Department to review the training plan and training materials, which shall give the Department an opportunity to validate the Contractor has met entrance and exit criteria for training, including implementation of the training environment and completion of all scheduled training sessions. The Contractor's Training Lead shall also participate in this meeting. The Contractor shall make updates to the Contractor's plans and materials as needed based on feedback from this walkthrough.

10.4.1.1. The Contractor shall present the approach to training Providers in the Communication Management Plan. This approach shall identify and address the specific needs of the Provider community and the final materials that will need to be distributed to the Providers as well as Provider outreach activities.

10.4.2. Requirement Stage: PBMS Implementation Contract Stage

10.5. Reference #2064: Maintain and update the training environment with training data to use during staff trainings.

10.5.1. Contractor Approach: The Contractor shall maintain and update a training environment with training data for staff training purposes. The training environment shall be made available for all training courses and documentation needs during the Operational Readiness Phase. The lead trainer, the training material, and the technical resources shall ensure all training requirements are established and met. The training environments and training data shall be refreshed as needed to provide training using current operational scenarios.

10.5.2. Requirement Stage: PBMS Implementation Contract Stage

10.6. Reference #2065: Provide regular refresher training sessions for authorized System users to disseminate updated or new functionality or business processes related to the PBMS throughout the Contract term, extending as agreed upon.

10.6.1. Contractor Approach: The Contractor shall be responsible for ensuring that all system users are made aware of updated or new functionality. The knowledge gaps shall be eliminated by providing regular refresher training and user documentation.

10.6.2. Requirement Stage: All Contract Stages

10.7. Reference #2066: Develop and submit for Department approval a Training Plan that meets the requirements described in this Exhibit.

10.7.1. Contractor Approach: The Contractor shall be responsible for the Training Plan as well as all training activities. The Training Plan and resulting training processes and documentation shall ensure that Contractor staff, Department staff, and any affected Department contractors are thoroughly and appropriately trained to be proficient in system functionality and to ensure efficient, effective business operations related to the PBMS. The Department will review and approve the Training Plan during the Organizational Readiness and Training Phase.

10.7.2. Deliverable: Training Plan

10.7.3. Deliverable Stage: PBMS Implementation Contract Stage

10.8. Reference #2067: The Resource Management Plan shall include a Training Plan to be reviewed annually and approved by the Department. The plan shall demonstrate the commitment of the Contractor staff to meet the learning needs of the authorized System users and include a proposed plan for face-to-face training on a mutually agreed upon schedule.

10.8.1. Contractor Approach: The Contractor shall provide a Resource Management Plan which contains a Training Plan that outlines the approach to meet Department staff and Provider training needs. The plan shall indicate which courses will be offered, the schedule, and method of delivery. Face-to-face training shall be offered to the Department staff on a mutually agreed upon schedule. These plans shall be updated annually, at a minimum, based on course evaluation results and collaboration between the Contractor and state staff. The Contractor shall update the Training Plan as needed to address changes in the PBMS and Services.

10.8.2. Deliverable: Training Plan

10.8.3. Deliverable Stage: PBMS Implementation Contract Stage

10.9. Reference #2068: As specified in the Training Plan, develop, deliver, update, maintain, and conduct a broad spectrum of comprehensive training programs including an evaluation and quality improvement component for all training sessions, and related documentation and materials, for initial and ongoing training for internal and external stakeholders, including, but not limited to, authorized PBMS users from the Department, providers, the Contractor, and other supporting contractors.

10.9.1. Contractor Approach: The Training Plan shall outline how the Contractor will use experience and industry expertise to address training needs for providers, Department staff, and Contractor staff. The Training Plan shall detail the approach, methodology, curriculum, and schedule that the Contractor will use to achieve a customized learning program and address the needs of the Department. The Contractor shall provide course evaluation forms to all stakeholders to complete which provide valuable feedback on course, training documentation, and instructor effectiveness.

10.9.2. Requirement Stage: All Contract Stages

11. COMMIT PROJECT PHASES, IMPLEMENTATION AND ROLL OUT PHASE

11.1. Reference #2069: Develop an Implementation Strategy in conjunction with the Department.

11.1.1. The Implementation Strategy shall describe, at a minimum:

11.1.1.1. The phased approach to the PBMS roll out to authorized PBMS user groups and/ or of functionality.

11.1.1.2. The proposed implementation schedule.

11.1.1.3. A tracking process for Problems and Defects.

11.1.1.4. Communication and Contractor support procedures.

11.1.1.5. Contractor and Department roles and responsibilities.

11.1.1.6. Operational Readiness Criteria and Operational Readiness Walkthrough approach that addresses Contractor and PBMS and Department readiness.

11.1.1.7. PBMS acceptance procedures.

11.1.2. Contractor Approach: As described in the Project Management Plan and its ancillary plans, the Contractor shall develop in conjunction with the Department a phased approach to the PBMS implementation across the 12 phases of the Contract.

11.1.2.1. The phased approach shall include an implementation schedule reviewed with the Department as outlined in the Communication Management Plan. The Contractor shall also develop a tracking process for Problems and Defects, support procedures, roles and responsibilities and the Operational Readiness Criteria.

11.1.2.2. The Operational Readiness Criteria shall include an Operational Readiness Walkthrough, and this shall include a review of the Contractors Operational Readiness Checklist.

11.1.2.3. PBMS acceptance procedures shall be outlined in the Project Management Plan and shall mimic the document approval procedures agreed upon by the Contractor and the Department to draft, review, revise and approve documents throughout the PBMS implementation.

11.1.3. Deliverable: Implementation Strategy

11.1.4. Deliverable Stage: PBMS Implementation Contract Stage

11.2. Reference #2070: Conduct an Operational Readiness Walkthrough with the Department prior to the initial PBMS Implementation and Roll Out Phase. The Operational Readiness Walkthrough shall validate the Contractor's, PBMS's, and Department's operational readiness. The Department shall formally sign off on each Operational Readiness Walkthrough prior to implementing the next Roll Out Phase.

11.2.1. Contractor Approach: The Contractor shall conduct an Operational Readiness Walkthrough with the Department prior to the initial PBMS Implementation and Rollout Phase.

11.2.1.1. The Operational Readiness Walkthrough shall include the review and verification of the readiness of the PBMS, Services and the Department for implementation.

11.2.1.2. The Contractor shall present a draft of Operational Readiness Checklist to the Department for review and comments to ensure all requirements are met and processes and systems are functioning correctly.

11.2.1.3. The RTM Gap Analysis shall be reviewed during these sessions in order to prioritize the gaps for closure. This meeting shall be intended to validate and close any outstanding issues before the deliverable is formally presented to the Department for review, approval and acceptance.

11.2.2. Deliverable: Operational Readiness Walkthrough and Checklist

11.2.3. Deliverable Stage: PBMS Implementation Contract Stage

11.3. Reference #2071: Develop a "Go-Live" Support Plan that documents the onsite and offsite authorized PBMS user support provided by the implementation. Go-Live is defined as the period when the Production Environment is first accessed by authorized PBMS users to support business functions to the time when the Department formally accepts the PBMS. The Go-Live support model is different than the Help Desk, which is meant to support the PBMS once operationally stable.

11.3.1. Contractor Approach: The Contractor shall develop a "Go-Live" Support Plan, with Department approval, that documents the onsite and offsite authorized PBMS user support provided by the implementation.

11.3.1.1. The Contractor shall proactively work with all switch vendors supporting pharmacies in the state to ensure they have configured their software properly, and can successfully execute test claims in the Contractor's test environment prior to "Go-Live".

11.3.1.2. Contractor shall coordinate with the switch vendors in the hours prior to "Go-Live" to ensure claims successfully transmit in the Contractor's POS production environment.

11.3.1.3. Once the POS system goes live, the Contractor shall monitor claims real time and produce hourly reports to evaluate adjudication results and target any providers experiencing a high volume of claims rejections.

11.3.2. Deliverable: "Go-Live" Support Plan

11.3.3. Deliverable Stage: PBMS Implementation Contract Stage

11.4. Reference #2072: Develop an Implementation and Roll Out Plan that details planning and roadmaps for managing all PBMS releases (if applicable). This includes managing dependencies across releases along with handling Technology Stacks, databases and infrastructure to match the roll out needs.

11.4.1. Contractor Approach: The Contractor shall have a systematic release management process in place for production information systems and technologies.

11.4.1.1. The Contractor's Change Management procedures shall be designed to ensure the effective process of planning, scheduling, communicating, and implementing changes successfully. The Contractor shall provide a Release Management Plan for the Department that satisfies the Department's release cycle

11.4.2. Deliverable: Implementation and Roll Out Plan

11.4.3. Deliverable Stage: PBMS Implementation Contract Stage

11.5. Reference #2073: Develop a Post-Implementation Operational Monitoring Plan, including methods and schedules for the Department and the Contractor to conduct post-implementation monitoring of PBMS Operations related to performance expectations as described in this Exhibit.

11.5.1. Contractor Approach: The Contractor shall develop a Post-Implementation Operational Monitoring plan, including methods and schedules for the Department and Contractor to conduct post-implementation monitoring of PBMS Operations related to performance.

11.5.1.1. The Contractor shall provide post-implementation reporting to the Department after a facility, function, or work group has been determined to be ready for production cutover in accordance with the Department approved scheduled time frames. For 30 calendar days following each operational and system implementation, the Contractor shall review the all aspects of the implementation to ensure the PBMS and operational processes are performing as expected and that nothing has adversely affected other processes. If defects are identified, they shall be immediately corrected and the corrections migrated to production.

11.5.1.2. A QA and production environment shall be maintained during the term of the Contract to allow for thorough testing prior to promotion to production. During this period, the project team shall solicit feedback necessary for continuous improvement of work processes and product.

11.5.2. Deliverable: Post-Implementation Operational Monitoring Plan

11.5.3. Deliverable Stage: PBMS Implementation Contract Stage

11.6. Reference #2074: Update System documentation and operating procedures with lessons learned from the Implementation and Roll Out Phase.

11.6.1. Contractor Approach: The Contractor's Pharmacy Services Account Manager shall modify operating procedures to reflect changes with Contractor PBMS Operations and shall document the lessons learned and modify operational procedures based on those lessons learned.

11.6.1.1. The Contractor shall upload and store all procedures in a centralized Procedure Documentation Library.

11.6.1.2. All authorized Department users shall have access to the Procedure Documentation Library for reference.

11.6.1.3. The Contractor shall review all procedures at least once per calendar year, or more often as needed to account for changes to the PBMS and Services, to ensure that all documentation is up-to-date. Owners of procedures shall receive notification prior to the review due date (typically two months prior) and are responsible for making any changes in procedures using Track Changes in Microsoft Word, updating the Revision History and describing changes as minor or major.

11.6.2. Requirement Stage: PBMS Implementation Contract Stage

11.7. Reference #2075: Obtain formal Department approval for the implementation of the System.

11.7.1. Contractor Approach: The Contractor shall seek and obtain formal department approval prior to implementation of the system.

11.7.2. Requirement Stage: PBMS Implementation Contract Stage

11.8. Reference #2076: Prepare a Post-Implementation Evaluation Report.

11.8.1. The Post-Implementation Evaluation Report shall include:

11.8.1.1. Lessons learned.

11.8.1.2. Project successes and failures.

11.8.1.3. Evaluation metrics including:

11.8.1.3.1. Actual and planned budget comparisons.

11.8.1.3.2. Actual and planned schedule comparisons.

11.8.1.3.3. Actual and planned scope comparisons.

11.8.1.4. Authorized PBMS user satisfaction.

11.8.1.5. Benefits gained over the previous System.

11.8.1.6. The current status of the System.

11.8.1.7. Ongoing contingencies or problems.

11.8.2. Contractor Approach: The Contractor shall deliver a post-implementation report categorized by content area after a facility, function, or work group has been determined to be ready for production cutover in accordance with the Department approved scheduled time frames.

11.8.3. Deliverable: Post-Implementation Evaluation Report

11.8.4. Deliverable Stage: PBMS Implementation Contract Stage

12. COMMIT PROJECT PHASES, OPERATIONS AND MAINTENANCE PHASE

12.1. Reference #2077: Perform operations and maintenance throughout the life of the Contract at no additional cost to the Department, and develop and make available electronically a PBMS Operations and Maintenance Plan.

12.1.1. The PBMS Operations and Maintenance Plan shall include the following:

12.1.1.1. Monitoring of daily performance.

12.1.1.2. Updates, patches, licenses, and repairs to components of the production, test, training, UAT, and all other accessible environments including but not limited to:

12.1.1.3. Hardware.

12.1.1.4. Operating Systems.

12.1.1.5. Database Systems.

12.1.1.6. Application and other software.

12.1.1.7. Utilities for Systems, database, software, communications.

12.1.1.8. Voice, video, data communication lines.

12.1.1.9. Communications software.

12.1.1.10. Drivers.

12.1.1.11. Configurations.

12.1.2. Contractor Approach: During the operations and maintenance phase, the Contractor shall deliver an Operations and Management Plan to the Department.

12.1.2.1. The plan shall outline the Contractor's standard approach to system maintenance and monitoring activities throughout the life of the Contract and shall include topics such as:

12.1.2.1.1. Monitoring of daily performance.

12.1.2.1.2. Updates, patches, licenses, and repairs to components of the production, test, training, UAT, and all other accessible environments including but not limited to hardware, operating systems, database systems, application and other software, utilities for systems, database, software, communications, voice, video, data communication lines, communications software, drivers, and configurations.

12.1.2.2. The standard system operations and maintenance activities shall be performed at no additional cost to the Department.

12.1.3. Deliverable: PBMS Operations and Maintenance Plan

12.1.4. Deliverable Stage: PBMS Ongoing Operations and Enhancements Contract Stage

12.2. Reference #2078: As defined by the PBMS Operations and Maintenance Plan the Contractor shall provide:

12.2.1. Defect identification, tracking, and correction process.

12.2.2. Plan for maintaining security on a database, network, and individual authorized System user level including maintenance of authorized System user accounts.

12.2.3. Contractor Approach: The PBMS Operations and Maintenance Plan shall define and communicate the Contractor's defect identification, tracking, and correction process. The plan shall provide details of its process workflow interaction with the JIRA section of the Atlassian suite of products to define, trace, verify and report all defects. Developers, Plan Administrators, and Testers shall be given access to JIRA to facilitate rapid awareness and response to a defect. Work around resolution processes, management controls, and Department oversight of the necessary steps to quickly remediate to the satisfaction of the Department shall be clearly identified and presented as part of the plan.

12.2.4. The Contractor's PBMS security approach shall be included in the PBMS Operations and Maintenance Plan and shall include operations for maintaining security on a database, network, and individual authorized PBMS user level including maintenance of authorized system user accounts.

12.2.5. Deliverable: PBMS Operations and Maintenance Plan

12.2.6. Deliverable Stage: PBMS Ongoing Operations and Enhancements Contract Stage

12.3. Reference #2079: As defined by the PBMS Operations and Maintenance Plan the Contractor shall also include a Help Desk Support Plan.

12.3.1. The Help Desk Support Plan shall include, at minimum:

12.3.1.1. Available support services and proposed help desk staffing model that will ensure the performance expectations detailed in this Exhibit.

12.3.1.2. Internal Contractor policies to ensure Protected Health Information (PHI), Personally Identifiable Information (PII) and other Department or client data is only shared with appropriate staff.

12.3.1.3. After-hour contact and problem reporting process.

12.3.1.4. System documentation, including end-user and System administrator documentation.

12.3.1.5. Proposed Contractor staffing model for the Operations Phase.

12.3.1.6. Process for submitting operations problem reports to the Department when operational problems occur, describing the nature of the problem, the expected impact on ongoing functions, a corrective action plan, and the expected time of problem resolution.

12.3.2. Contractor Approach: Contractor shall provide a live pharmacy help desk available twenty-four (24) hour a day and seven (7) days a week through a toll-free number for Department and authorized users. Contractor shall allow the option for authorized users to leave a voicemail if the help desk agent is busy. The process for submitting operations problem reports to the help desk and the process through which they will be addressed shall be documented in the PBMS Operations and Maintenance Plan. The help desk shall:

12.3.2.1. Perform initial investigation, impact assessment, and prioritization on all requests

12.3.2.2. Forward non-System related issues to the appropriate Department or Contractor staff

12.3.2.3. Escalate issues as defined in the Operations and Maintenance Plan.

12.3.2.4. Be appropriately staffed according to the staffing model outlined in the Operations and Maintenance Plan with respect to performance expectations.

12.3.2.5. Abide by all of the Contractor's security policies including but not limited to the areas of Protected Health Information and Personal Identifiable Information.

12.3.2.6. Have access to the shared document repository to retrieve all end user and system administrator documentation

12.3.3. Deliverable: Help Desk Support Plan

12.3.4. Deliverable Stage: All Contract Stages

12.4. Reference #2080: Publish a System Software Version Release Schedule and provide updates to the Department as requested.

12.4.1. Contractor Approach: The Contractor shall publish onto the shared document repository a System Software Version Release Schedule. The schedule shall include

updates planned for deployment to any of the components of the PBMS, both application and infrastructure. Application updates shall contain enhancements and issue mediations that have come through the Contractor's change management systems which includes testing and prioritization collaboration with the Department. Infrastructure updates shall include but are not limited to operation system patches, and data base management system updates. Updates to the schedule shall be posted the shared document repository which shall be accessible by authorized Department users.

12.4.2. Deliverable: System Software Version Release Schedule

12.4.3. Deliverable Stage: PBMS Ongoing Operations and Enhancements Contract Stage

12.5. Reference #2081: Provide online end user and System Administrative Documentation that includes, at minimum, information on System screens, workflows, data fields, reports.

12.5.1. Contractor Approach: The Contractor shall provide end user and System Administrative Documentation by uploading it to the shared document repository. This documentation shall include but not be limited to information on system screens, workflows, data fields, and reports. As enhancements are made to support specific aspects of the program, updates to the documentation shall occur and be posted to the shared document repository as part of the Contractor's deployment process. Documents in the shared document repository shall be accessible to authorized Department users.

12.5.2. Deliverable: End User and System Administrative Documentation

12.5.3. Deliverable Stage: PBMS Ongoing Operations and Enhancements Contract Stage

12.6. Reference #2082: Provide secure and encrypted email account(s) for the Department to report problems, questions or PBMS problems while safely exchanging PHI/ PII, as required.

12.6.1. Contractor Approach: The Contractor shall enable a method of delivering secure e-mail communications. This secure email system shall allow for the Department to report problems, questions or PBMS problems while safely exchanging PHI/ PII, as required. The method shall involve the use of Virtual Private Networks (VPN), an encrypting e-mail gateway, a Web-based secure e-mail service and employee or contractor training and awareness. The Contractor's external e-mail communications layer supported shall include Transport Layer Security (TLS) protocol version 1.0 /Secure Socket Layer (SSL) protocol version 3.0 known here as TLS/SSL using Advanced Encryption Standards (AES) minimum 128-Bit keys.

12.6.2. Requirement Stage: PBMS Ongoing Operations and Enhancements Contract Stage

12.7. Reference #2083: Provide a searchable library, with highly flexible search criteria (e.g., single character and string wildcard searches) to enable an authorized PBMS user to quickly find needed information in policy manuals, training material, implementation memos and all necessary help functions.

12.7.1. Contractor Approach: The Contractor shall use a document management system, which provides a unified general content management solution that supports versioning capabilities and appropriate change control. The document library shall be easily configurable to organize documentation so that it is easy to find. The library also shall be supported by full text search capability for text based documents, enabling document

consumers to quickly and easily track down the information they are searching for. The Contractor shall provide access to authorized PBMS users to search information for policy manuals, training material, implementation memos and all necessary help functions.

12.7.2. Requirement Stage: PBMS Ongoing Operations and Enhancements Contract Stage

12.8. Reference #2084: There shall be a Warranty Period, as defined in the Contract.

12.8.1. Contractor Approach: The Contractor shall provide a warranty period that shall last through the first 365 calendar days of the PBMS Ongoing Operations and Enhancement Contract Stage. The warranty shall cover the agreed-upon functionality. The Contractor shall be responsible for keeping the PBMS operating according to Department specifications. Any Defects identified and accepted through the Change Management Process shall be addressed by the Contractor with no additional cost to the Department. The PBMS performance and operations shall continue while the defects are being addressed.

12.8.2. Requirement Stage: PBMS Ongoing Operations and Enhancements Contract Stage

13. COMMIT PROJECT PHASES, CMS CERTIFICATION PHASE

13.1. Reference #2085: Coordinate with the Department to develop Centers for Medicare and Medicaid Services (CMS) Certification Checklist documentation for each Medicaid Enterprise Certification Toolkit (MECT) Checklist requirement.

13.1.1. Contractor Approach: The Contractor shall coordinate with the Department in regard to selecting, tailoring, and completing all checklists that apply to the PBMS and Services.

13.1.1.1. Contractor shall use software designed to assist tracking and completion of the toolkits/MECT

13.1.2. Deliverable: Documentation for each MECT Checklist requirement

13.1.3. Deliverable Stage: PBMS Ongoing Operations and Enhancements Contract Stage

14. COMMIT PROJECT PHASES, ENHANCEMENT PHASE

14.1. Reference #2086: Develop an Enhancements Test Plan that describes the approach to all testing necessary to implement Enhancements.

14.1.1. Contractor Approach: The Contractor shall develop an Enhancements Test Plan that describes the approach to all testing necessary to implement Enhancements. The Contractor's typical process for testing enhancements shall include at least the following steps:

14.1.1.1. Requirement review and clarification -This allows the tester to fully understand the desired outcome of the change being made. Participants shall include at least the following: Department staff if desired, Contractor business analyst, test lead/tester, developer or configuration staff.

14.1.1.2. Test case development and prep - The prep involves populating the case with actual Department data

14.1.2. Deliverable: Enhancement Test Plan

14.1.3. Deliverable Stage: PBMS Ongoing Operations and Enhancements Contract Stage

14.2. Reference #2087: Design, implement, and document detailed test cases (UAT initial test cases and detailed PBMS test cases) for Enhancement testing. Test cases shall include dummy IDs (not real ones), detailed steps, expected results, actual results (where appropriate), and be traceable to requirements listed in this Contract in the RTM.

14.2.1. Contractor Approach: The Contractor shall design, implement and document detailed test cases (UAT and initial test cases and detailed PBMS test cases for Enhancement testing.) Test cases documentation shall include at least dummy/test IDs, detailed steps, expected and actual results, and shall be traceable to the RTM.

14.2.2. Deliverable: Detailed Test Cases

14.2.3. Deliverable Stage: PBMS Ongoing Operations and Enhancements Contract Stage

14.3. Reference #2088: Submit all Test Results for each test sub-phase to the Department.

14.3.1. The Test Results shall include, at minimum:

14.3.1.1. Summary of testing results.

14.3.1.2. Pass/ Failure Rate.

14.3.1.3. Defect IDs and severity level of failed test cases.

14.3.1.4. Proposed resolution for identified defects.

14.3.1.5. Performance/ Stress Testing Results.

14.3.1.6. Final Enhancements Test Results.

14.3.1.7. Penetration Test Results.

14.3.2. The following tests shall be done independently with the results, defects and severity level, pass/ fail rate, and proposed resolution for identified defects submitted to the Department:

14.3.2.1. Performance/ Stress Testing.

14.3.2.2. Final Enhancements Test Results.

14.3.2.3. Penetration Test Results.

14.3.3. Contractor Approach: All tester results shall be submitted by the Contractor to the Department.

14.3.3.1. The Contractor shall include at minimum:

14.3.3.1.1. Summary of testing results.

14.3.3.1.2. Pass/ Failure Rate.

14.3.3.1.3. Defect IDs and severity level of failed test cases.

14.3.3.1.4. Proposed resolution for identified defects.

14.3.3.1.5. Performance/ Stress Testing Results, if necessary.

14.3.3.1.6. Final Enhancements Test Results.

14.3.3.1.7. Penetration Test Results, if necessary.

14.3.3.2. The Performance/Stress Testing, Final Enhancement Testing, and Penetration testing shall be done independently, and the results (including items above) shall be submitted to the Department.

14.3.4. Deliverable: Test Results

14.3.5. Deliverable Stage: PBMS Ongoing Operations and Enhancements Contract Stage

14.4. Reference #2089: Collaborate with the Department to identify and prioritize its PBMS requirements that are not included in the base PBMS and are outside of the contracted scope, following the Change Management Process.

14.4.1. Contractor Approach: The Contractor shall evaluate the reasonableness and complexity of the change, communicate the level of effort and shall work closely with the Department to ensure change requests are accurately prioritized. The change request shall then be attached to a ticket in the Contractor's requirement management and tracking tool.

14.4.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

15. COMMIT PROJECT PHASES, TURNOVER PHASE

15.1. Reference #2090: Develop a PBMS Turnover Plan at no additional cost to the Department.

15.1.1. The PBMS Turnover Plan shall include, at minimum:

15.1.1.1. Proposed approach to Turnover.

15.1.1.2. Tasks and subtasks for Turnover.

15.1.1.3. Schedule for Turnover.

15.1.1.4. Entrance and exit criteria.

15.1.1.5. Readiness walkthrough process.

15.1.1.6. Documentation update procedures during Turnover.

15.1.1.7. Description of Contractor coordination activities that will occur during the Turnover Phase that will be implemented to ensure continued functionality of PBMS and services as deemed appropriate by the Department.

15.1.2. Contractor Approach: To deliver an orderly and timely turnover, the Contractor shall provide an updated, comprehensive Project Turnover and Closeout Project Plan descriptive of the methodology used in the execution the Contract with the Department for review and approval.

15.1.2.1. Contractor shall provide a designated Turnover Coordinator during this phase to work with the incoming vendor. This Turnover Coordinator shall establish a collaborative relationship with the new vendor and the Department to perform the critical tasks of transitioning the program. Contractor shall provide the Department with an initial Turnover Plan and Service plan during Phase I – Project Planning and Startup, at no additional cost to the Department. This plan, led by the turnover project manager, shall be updated throughout the Contract term as necessary to retain the Contractor's contractual obligation and scope of services current. The

Turnover Project Plan shall include all tasks, subtasks activities, milestones, and deliverables; turnover status reports; and input responsibilities to the Department. Contractor shall assign a full-time turnover coordinator from the beginning of the turnover phase until termination of the Contract.

15.1.3. Deliverable: PBMS Turnover Plan

15.1.4. Deliverable Stage: PBMS Ongoing Operations and Enhancement Contract Stage

15.2. Reference #2091: Develop a System Requirements Statement at no additional cost that would be required by the Department or another designee to fully take over the System, technical, and business functions outlined in the Contract. The Statement shall also include an estimate of the number, type, and salary of personnel required to perform the other functions of the System. The Statement shall be separated by type of activity of the personnel.

15.2.1. The Statement shall include all facilities and any other resources required to operate the System, including, but not limited to:

15.2.1.1. Telecommunications networks.

15.2.1.2. Office space.

15.2.1.3. Hardware.

15.2.1.4. Software.

15.2.1.5. Other technology.

15.2.2. The Statement shall be based on the Contractor's experience in the operation of the PBMS and shall include actual Contractor resources devoted to operations activities.

15.2.3. Contractor Approach: The Contractor shall review and analyze all requirements pertaining to the operations, maintenance and delivery necessary to fully take over the system, technical, and business functions outlined in the Contract. The Contractor shall provide a resources and staffing plan that guarantees a sufficient number of experienced staff to perform the work for system development, operations and maintenance, claims/encounters processing, system engineering, documentation and training, project management, contact center and help desk services to properly administer the PBMS.

15.2.3.1. The Resource Management Plan shall contain the following:

15.2.3.1.1. A description of the proposed organization for each of the Project Phases of the Contract

15.2.3.1.2. An Organization Chart that identifies positions

15.2.3.1.3. Position descriptions and qualifications for each Labor Category identified on the proposed organization charts

15.2.3.1.4. A link or reference to the Department approved Training Plan that demonstrates the commitment of the Contractor staff to meet the learning needs of the authorized System users and include a proposed plan for face-to-face training on a mutually agreed upon schedule

15.2.3.1.5. Information for each position that shall include at least:

15.2.3.1.6. Labor Category title

15.2.3.1.7. Position description

15.2.3.1.8. Required education, training, licensure, and certification

15.2.3.1.9. Required experience

15.2.3.1.10. Specific skills or knowledge required.

15.2.4. Deliverable: System Requirements Statement

15.2.5. Deliverable Stage: PBMS Ongoing Operations and Enhancement Contract Stage

15.3. Reference #2092: Provide a Lessons Learned Document that describes valuable lessons learned during the COMMIT project.

15.3.1. Contractor Approach: The Contractor's project team shall develop a lessons learned document during implementation that the Contractor shall build on throughout the project. Lessons learned shall be documented at the completion of each project phase. The Contractor shall provide a written progress report to include an Issues/Risks section. These identified risks/issues shall serve as documentation for lessons learned.

15.3.1.1. Contractor shall apply these lessons learned from this project and other projects to develop improved processes within the Colorado operations.

15.3.2. Deliverable: Lessons Learned Document

15.3.3. Deliverable Stage: PBMS Ongoing Operations and Enhancement Contract Stage

16. PBMS OPERATIONS, OPERATIONS TRANSITION PLANNING PHASE

16.1. Reference #2093: Develop and submit a Transition Plan.

16.1.1. The Transition Plan shall include, at minimum:

16.1.1.1. Proposed approach to transition.

16.1.1.2. Proposed approach for conducting a knowledge transfer from the Contractor to the new contractor.

16.1.1.3. Proposed approach for consolidating applicable sections from the Contractor's Turnover Plan into the transition planning activity.

16.1.1.4. Tasks and activities for transition.

16.1.1.5. Personnel and level of effort in hours.

16.1.1.6. Completion date.

16.1.1.7. Transition Milestones.

16.1.1.8. Entrance and exit criteria.

16.1.1.9. Schedule for transition.

16.1.1.10. Production program and documentation update procedures during transition.

16.1.1.11. Readiness walkthrough.

16.1.1.12. Parallel test procedures.

16.1.1.13. Provider training.

16.1.1.14. Interface testing.

16.1.2. The Contractor shall execute the Transition Plan and activities at no additional cost.

16.1.3. Contractor Approach: The Contractor shall provide a Transition Plan that includes all requirements of this section.

16.1.4. Deliverable: Transition Plan

16.1.5. Deliverable Stage: PBMS Implementation Contract Stage

16.2. Reference #2094: Develop and submit a Relocation Risk/ Contingency Plan.

16.2.1. The Plan shall include:

16.2.1.1. Proposed approach to Contractor relocation risk/ contingency planning.

16.2.1.2. Risk analysis: identification of critical business processes.

16.2.1.3. Risk analysis: identification of potential failures.

16.2.1.4. Risk analysis: business impacts.

16.2.1.5. Identification of alternatives/ contingencies.

16.2.2. Contractor Approach: The Contractor shall Develop and submit a Relocation Risk/ Contingency Plan. All predecessor and successor dependencies for relationship separation shall be captured in the work plan to ensure there will be no interruption of services or quality of care to the Department's population. The plan shall demonstrate the Contractor's stepwise approach to determining the necessary processes to fully take over the PBMS and Services. The plan shall outline the risk analyses completed for: identification of critical business processes; identification of potential failures; business impacts and identification of alternates/contingencies for the same.

16.2.3. Deliverable: Relocation Risk/ Contingency Plan

16.2.4. Deliverable Stage: PBMS Implementation Contract Stage

17. PBMS OPERATIONS, OPERATIONS PARALLEL TESTING PHASE

17.1. Reference #2095: Establish a Parallel Test Plan that describes the Contractor's approach to conducting the parallel test.

17.1.1. The Parallel Test Plan shall include, at minimum:

17.1.1.1. Role and responsibilities.

17.1.1.2. Proposed activities and procedures.

17.1.1.3. Proposed timeline.

17.1.1.4. Proposed reporting structure.

17.1.1.5. Supporting tools and documentation to support the Parallel Test.

17.1.2. Contractor Approach: The Contractor shall create a Parallel Test Plan that describes the Contractor's approach to conducting the parallel testing, including, at minimum:

17.1.2.1. Purpose of the Parallel test and expected outcomes

17.1.2.2. Role and responsibilities.

17.1.2.3. Scope and definition of the parallel test,

17.1.2.4. Proposed activities and procedures.

17.1.2.5. Proposed timeline.

17.1.2.6. Proposed reporting structure.

17.1.2.7. Supporting tools and documentation to support the Parallel Test.

17.1.3. The Parallel Test shall be designed to identify the natural discrepancies between the Legacy system and the Contractor's system, as well as true defects that must be resolved prior to release to production.

17.1.4. Deliverable: Parallel Test Plan

17.1.5. Deliverable Stage: PBMS Implementation Contract Stage

17.2. Reference #2096: Perform parallel test of the PBMS with input from the incumbent contractor’s operations and report test results to the Department.

17.2.1. Contractor Approach: According to the parallel test plan, the Contractor shall perform the parallel test in collaboration with the incumbent contractor.

17.2.2. Requirement Stage: PBMS Implementation Contract Stage

17.3. Reference #2097: Revise System and user documentation as required to fully describe the Contractor’s operations.

17.3.1. Contractor Approach: The Contractor shall provide updated System and User documentation to the Department that shall completely describe the Contractor's operations. In addition to standard user documentation, the Contractor shall also provide job aides that provide summarized quick reference material for end users.

17.3.2. Requirement Stage: All Contract Stages

18. PBMS OPERATIONS, OPERATIONAL READINESS PHASE

18.1. Reference #2098: Modify operating procedures to reflect changes with Contractor operations.

18.1.1. Contractor Approach: The Contractor shall modify operating procedures to reflect changes in the Contractor’s PBMS operations. The Contractor’s staff shall upload and store all procedures in a centralized Procedure Documentation Library, and all designated employees shall have access to the Procedure Documentation Library for reference.

18.1.1.1. The Contractor shall review all procedures at least once per year, or as needed to account for any changes to the PBMS and Services to ensure that all documentation is updated/modified and reflects current operations. Owners of procedures shall receive notification prior to the review due date (typically two months prior) and are responsible for making any changes in procedures using Track Changes in Microsoft Word, updating the Revision History and describing changes as minor or major.

18.1.2. Requirement Stage: All Contract Stages

18.2. Reference #2099: Develop or revise provider manuals to reflect changes with Contractor operations using a variety of notification methods including Web Portal, email, and/ or provider bulletin mailings.

18.2.1. Contractor Approach: The Contractor shall create a Provider Training Manual which shall cover all aspects of the PBMS and PA processes during the Operational Readiness Phase. All provider communications including the provider manuals shall be maintained and distributed to the provider community via mail, fax, or email by the Contractor. In addition, the Contractor shall provide information to the Department for the Department to post to its website or web portal, including provider bulletins, revised training materials and provider manuals.

18.2.1.1. The Contractor's Training Lead shall be responsible for updating the Provider Manual to reflect any changes made during the Operations phase that affects how pharmacy claims and prior authorizations are processed.

18.2.2. Requirement Stage: All Contract Stages

18.3. Reference #2100: Develop a Department Operational Readiness Training Plan and conduct training for Department staff in order to ensure preparedness for operations.

18.3.1. Contractor Approach: The Contractor shall develop a Department Operational Readiness Training Plan, in collaboration with the Department, to address all training needs and facilitate all training for Department staff to ensure preparedness for operations.

18.3.2. Deliverable: Department Operational Readiness Training Plan

18.3.3. Deliverable Stage: PBMS Implementation Contract Stage

18.4. Reference #2101: Conduct a formal Operational Readiness Plan Walkthrough with the Department, demonstrating that all operational areas are ready.

18.4.1. Contractor Approach: The Contractor shall conduct an Operational Readiness Plan Walkthrough with the Department to demonstrate that all operational areas are ready for "Go-Live" of the PBMS and Services.

18.4.2. Deliverable: Operational Readiness Plan Walkthrough

18.4.3. Deliverable Stage: PBMS Implementation Contract Stage

18.5. Reference #2102: Prepare a final Operational Readiness Assessment Document, including results of the parallel test and an assessment of the final operational readiness of Contractor.

18.5.1. Contractor Approach: The Contractor shall prepare a final Operational Readiness Assessment Document, including results of the parallel test and an assessment of the final operational readiness.

18.5.1.1. The Contractor shall provide the Department with a Project phase Completion Report as a deliverable, which shall signify the acceptance by the Department of formal completion of each Phase.

18.5.1.2. Contractor shall employ a "Gate" concept with clearly defined entrance and exit criteria to demonstrate completion of a particular phase within the project lifecycle.

The "Gate" concept shall be a straightforward process used in conjunction with the Project Management Plan to help manage the balance among functionality and quality. Each "Gate" shall result in the certification that all appropriate work artifacts required to move forward to subsequent project activities have been completed, reviewed and meet quality expectations.

18.5.2. Deliverable: Operational Readiness Assessment Document

18.5.3. Deliverable Stage: PBMS Implementation Contract Stage

19. PBMS OPERATIONS, OPERATIONS IMPLEMENTATION AND START OF OPERATIONS PHASE

19.1. Reference #2103: Provide attestation to the Department that the System is operation-ready.

19.1.1. Contractor Approach: The Contractor shall provide this attestation to the Department when the PBMS is operation-ready.

19.1.2. Deliverable: Attestation the System is operation-ready

19.1.3. Deliverable Stage: PBMS Implementation Contract Stage

20. PBMS OPERATIONS, PBMS OPERATIONS

20.1. Reference #2104: Update Requirements Specifications for Approved Change Requests.

20.1.1. Contractor Approach: The Contractor shall update Requirements Specifications for approved change requests. The Contractor's Change Management Process shall include Contractor review and Department approval of all Change Requests and proposed implementation schedules. The Pharmacy Services Account Manager shall consult with the appropriate Operations and/or IT staff to determine if the request is included as part of the existing Contract or if a separate Statement of Work (SOW) is required. If a separate SOW is required, then one shall be prepared and submitted to the Department, and work shall commence once the SOW has been mutually agreed-upon and signed by both parties. If the agreed upon SOW includes additional funding or payment beyond that already included in the Contract, then work shall not commence on the SOW, and the Contractor shall not be paid for that SOW, until the SOW is formally added to the Contract through a Contract amendment or additional Customization and Configuration hours have been added through an Option Letter.

20.1.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

20.2. Reference #2105: Submit detailed Monthly Status reports, to be provided to the Department within seven (7) Business Days following the close of the month.

20.2.1. The Monthly Status Report shall include:

20.2.1.1. Progress toward achieving goals stated in the business plan.

20.2.1.2. Activities, by each function or unit of the Contractor organization (e.g., Pharmacy claims/ encounters, call center).

20.2.1.3. Achievement of performance standards for the previous month and identify all performance standards that were not met.

20.2.1.4. A summary of Contractor activities and key volume indicators, cumulative to the fiscal year end.

20.2.2. Contractor Approach: The Contractor shall provide the Department with a monthly status report within seven (7) Business Days after the end of each calendar month.

20.2.2.1. The Contractor shall meet in person with the Department, unless otherwise agreed to by the Department, to review a biweekly performance scorecard report (project status report) that tracks and reports on all required aspects of the work performed by the Contractor during the course of the Contract.

20.2.2.2. This performance score card shall be part of a single score card structure to track the health of the entire Colorado PBMS Project — staffing, operational volumes, SLA metrics, status of Department requests, and adherence to Department policies and procedures. There shall be a focus on current status, as well as forward-looking recommendations based on trends that are identified through the course of the Contract.

20.2.2.3. At a minimum, the Status Report shall include: Progress toward achieving goals stated in the business plan; activities by each function or unit of the Contractor organization (e.g., Pharmacy claims/encounters, and call center); achievement of performance standards for the previous month and identification of all performance standards that were not met; a summary of Contractor activities and key volume indicators, cumulative to the fiscal year end.

20.2.2.4. Exact analytics shall be defined with collaboration between the Department and the Contractor during the planning phase and throughout the life of the Contract based on changing needs and customer requests.

20.2.3. Deliverable: Monthly Status Report

20.2.4. Deliverable Stage: PBMS Ongoing Operations and Enhancement Contract Stage

20.3. Reference #2106: Develop and provide Modification/ Change Request Forms.

20.3.1. Contractor Approach: The Contractor shall create a change request form that outlines the requested modification/change.

20.3.2. Deliverable: Modification/ Change Request Forms

20.3.3. Deliverable Stage: PBMS Ongoing Operations and Enhancement Contract Stage

20.4. Reference #2107: Provide Updated Procedures and PBMS Documentation, as needed.

20.4.1. Contractor Approach: All requested changes shall be analyzed and processed through the Contractor's change management process. As part of this process, the impact of all aspects of PBMS shall be evaluated before approval is granted. When changes are performed that require updates to procedures and PBMS documentation, the Contractor shall complete the updates and submit for review and approval of all changes requested to the documentation.

20.4.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

20.5. Reference #2108: Develop and provide an Ongoing Support Maintenance Plan.

20.5.1. Contractor Approach: During the operations and maintenance phase, the Contractor shall deliver an Ongoing Support and Maintenance Plan to the Department.

20.5.1.1. The plan shall outline the Contractor's standard approach to system maintenance and monitoring activities throughout the term of the Contract and shall include:

20.5.1.1.1. Monitoring of daily performance.

20.5.1.1.2. Updates, patches, licenses, and repairs to components of the production, test, training, UAT, and all other accessible environments including but not limited to hardware, operating systems, database systems, application and other software, utilities for systems, database, software, communications, voice, video, data communication lines, communications software, drivers, and configurations.

20.5.1.2. The standard system operations and maintenance activities shall be performed at no additional cost to the Department.

20.5.2. Deliverable: Ongoing Support Maintenance Plan

20.5.3. Deliverable Stage: PBMS Ongoing Operations and Enhancement Contract Stage

21. PERFORMANCE STANDARDS AND EXPECTATIONS

21.1. Reference #2109: Report on all performance standards as specified in the Contract, as specified by the Communication Management Plan.

21.1.1. Contractor Approach: The Contractor shall report on all performance standards as specified in the Contract and as specified by the Communication Management Plan.

21.1.1.1. The Contractor shall work with project stakeholders to identify and track critical performance indicators that will provide management insight into the overall efficiency and effectiveness of the project.

21.1.1.2. The Contractor‘s Project Status Reporting includes status updates on the following:

21.1.1.2.1. Project Work Plan

21.1.1.2.2. Work Breakdown Structure (WBS)

21.1.1.2.3. Key Assumptions

21.1.1.2.4. Risk and risk avoidance

21.1.1.2.5. Project Management Plan

21.1.1.2.6. Corrective Action Plans (CAPs) and progress.

21.1.1.3. The project status reports shall be provided to the Department 10 days after the Effective Date and weekly thereafter. The Contractor's project status reporting shall include a weekly project status meeting and shall include all project stakeholders as identified during the Project Kick-off Meeting. The standing agenda for project status meetings shall include the overall health of the project and a discussion of issues or risks that may affect the schedule, budget, or deliverables during each phase of this project.

21.1.1.4. The Contractor shall also be responsible for creating meeting minutes, project control and management plan, transmittal process, project calendar, user security access document, deliverables list, transmittal log, status reports, Change Control Board documents, project metrics, and for coordinating daily testing meetings.

21.1.2. Deliverable: Performance Standard Report

21.1.3. Deliverable Stage: PBMS Implementation Contract Stage

22. LOCATION OF CONTRACT FUNCTIONS AND PERSONNEL

22.1. Reference #2110: The Contractor shall maintain a facility that shall be located within walking distance, a one- (1-) mile radius of the Department, and accessible by public transportation, in a location approved by the Department.

22.1.1. Contractor Approach: The Contractor shall provide a local site in Denver with facilities within one mile of the Department to accommodate collaboration, project planning, and other DDI activities, as needed, and for all Contract Stages. These facilities shall be accessible by public transportation, approved by the Department, and could include a sublet from the MMIS Contractor. Both The Contractor's Pharmacy Services Account Manager and Pharmacy Systems Manager shall be located in this facility. During implementation, the DDI Project Manager shall spend a significant amount of time in Denver leading the project team to ensure successful, timely completion of project deliverables and seamless communications and shall work out of the Contractor's Denver facility. The remainder of the time, the DDI Project Manager shall be located off-site. Corporate resources shall be orchestrated and communicated with as needed.

22.1.2. Requirement Stage: All Contract Stages

22.2. Reference #2111: The Contractor shall have business hours from 8:00 am to 5:00 pm Mountain Time, each Business Day.

22.2.1. Contractor Approach: The Contractor shall have business hours from 8:00 a.m. to 5:00 p.m. Mountain Time, each Business Day.

22.2.1.1. During implementation, The Pharmacy Services Account Manager and DDI Project Manager shall be the main points of contact for the Department. They or a designee shall be available to the Department seven days a week, 24 hours a day. Pharmacy Support Center staff shall offer services 24 hours a day, seven days a week, 365 days per year, including holiday periods. During the Operations Stage, the Pharmacy Services Account Manager shall be the main point of contact.

22.2.2. Requirement Stage: All Contract Stages

22.3. Reference #2112: The Contractor shall supply sufficient meeting space at the Contractor's facility with WIFI access at their facility to satisfy the requirements of the Contract. The WIFI shall provide enough bandwidth to allow, and no security limitations that would prevent, the Department Staff to connect into their Virtual Private Network (VPN) from their State-issued laptops into the Department's network.

22.3.1. Contractor Approach: The Contractor shall supply meeting space to accommodate at least 20 people at the Contractor's facility (to include space for training and meetings).

This space shall provide wireless internet access equipped with enough bandwidth and security parameters to allow Department staff to connect into their Virtual Private Network (VPN) from their State-issued laptops.

22.3.2. Requirement Stage: All Contract Stages

22.4. Reference #2113: The Contractor shall supply one (1) workstation (or cubicles) at the Contractor's facility with WIFI access for the Department Staff use. The WIFI shall provide enough bandwidth to allow, and no security limitations that would prevent, the Department Staff to connect into their VPN from their State-issued laptops into the Department's network.

22.4.1. Contractor Approach: The Contractor shall supply a minimum of one (1) workstation with sufficient cubicle space at the Contractor's facility with WIFI access for Department staff use. The WIFI network shall provide sufficient bandwidth to allow, without restrictive security limitations that would prevent the Department Staff to connect into their VPN from their State-issued laptops into the Department's network.

22.4.2. Requirement Stage: All Contract Stages

23. CONTRACT PERSONNEL

23.1. Reference #2114: During the PBMS Implementation Contract Stage, ensure that certain personnel reside locally at the Contractor's facility.

23.1.1. All of the following resources shall reside locally at the Contractor's facility during the PBMS Implementation Contract Stage.

23.1.1.1. Pharmacy Services Account Manager.

23.1.2. Contractor Approach: The Contractor shall provide a Pharmacy Services Account Manager that shall reside locally at the Contractor's facility during the PBMS Implementation Contract Stage.

23.1.2.1. The Contractor's Business Analyst and Project Management support resources shall work on program activities at Contractor's headquarters outside of Colorado and shall make all necessary trips to attend on site meetings in Colorado during the PBMS Implementation Contract Stage in order to meet deliverables and ensure a successful implementation.

23.1.3. Requirement Stage: PBMS Implementation Contract Stage

23.2. Reference #2115: During PBMS Ongoing Operations and Enhancements Contract Stage, ensure that certain personnel reside locally at the Contractor's facility.

23.2.1. All of the following resources shall reside in the state at the Contractor's facility during the PBMS Ongoing Operations and Enhancements Contract Stage.

23.2.1.1. Pharmacy Services Account Manager.

23.2.1.2. Pharmacy Systems Manager.

23.2.2. Contractor Approach: The Contractor shall provide a Pharmacy Services Account Manager and Pharmacy Systems Manager who shall reside locally at the Contractor's facility during the PBMS Ongoing Operations and Enhancements Contract Stages.

23.2.3. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stages

23.3. Reference #2116: Provide a Resource Management Plan.

23.3.1. The Resource Management Plan shall include:

23.3.1.1. A description of the proposed organization for each of the Project Phases of the Contract described in Exhibit D, Project Phases.

23.3.1.2. An Organization Chart that identifies positions.

23.3.1.3. Position descriptions and qualifications for each Labor Category identified on the proposed organization charts.

23.3.1.4. A link or reference to the Department approved Training Plan that demonstrates the commitment of the Contractor staff to meet the learning needs of the authorized System users and include a proposed plan for face-to-face training on a mutually agreed upon schedule.

23.3.2. Contractor Approach: The Resource Management Plan shall be a component of the pharmacy implementation Project Management Plan, and shall include a description of the resource needs for each of the 12 phases of the pharmacy implementation. The Implementation Project Management Plan shall be presented by the Contractor to the Department during the implementation kick-off meeting. Following approval of the Implementation Project Management Plan, the Contractor shall develop an all-inclusive Resource Management Plan covering the 12 phases of the pharmacy implementation. The Resource Management Plan shall be developed during the Initiation and Planning phase and shall be approved prior to the start of the Discover and Requirements Validation / Requirements Elicitation Phase. The Resource Management Plan shall be updated through a progressive elaborative approach throughout the pharmacy implementation. The Contractor and Department shall review the Resource Management Plan in each of the 12 phases of the Contract. The Resource Management Plan shall include an organizational chart, and in conjunction with the Project Work Plan and the implementation strategy, as designed by the DDI Project Manager, the Resource Management Plan shall name those responsible for leading each workstream within each of the 12 phases of the Contract. For each person named as a lead within the Resource Management Plan, the plan shall include a description of each position, a description of each person's role and responsibility and their qualifications, as well as a link to the Contractor's training plan to ensure each person named can fully meet their obligations to the Department.

23.3.2.1. For any required component of this plan that is due in a later phase, the Contractor may note that component is due in that later phase and will be included in that phase.

23.3.3. Deliverable: Resource Management Plan

23.3.4. Deliverable Stage: All Contract Stages

23.4. Reference #2117: The Resource Management Plan shall also include information for each position.

23.4.1. This additional information shall include at least:

23.4.1.1. Labor Category title.

23.4.1.2. Position description.

23.4.1.3. Required education, training, licensure, and certification.

23.4.1.4. Required experience.

23.4.1.5. Specific skills or knowledge required.

23.4.2. Contractor Approach: The Resource Management Plan shall include a biography for each of the named positions. Each biography shall include the person's Labor Category title, a description of their position, the person's education, training, licensure and certification, a description of the person's experience and any skills or knowledge applicable to the person's role. The Contractor shall review each named position with the Department throughout the pharmacy implementation and at least once in each of the 12 implementation phases to ensure the requirements of this Contract are being met by those identified. The Resource Management Plan shall be a living document, initially approved by the Department during the Initiation and Planning phase, but revisited in each of the 12 implementation phases where additional resource biographies may be added by the Contractor or the Department to ensure the pharmacy implementation is being properly managed to meet the requirements of the Contract.

23.4.3. Deliverable: Resource Management Plan

23.4.4. Deliverable Stage: PBMS Implementation Contract Stage

23.5. Reference #2118: The Resource Management Plan shall also include additional information.

23.5.1. The additional information in the Resource Management Plan shall include:

23.5.1.1. A strategy for the organizational structure and team location(s) (specify in-state or out-of-state), and how this structure will contribute to project success.

23.5.1.2. A description for maintaining appropriate staffing levels throughout the term of the Contract and adjusting its resources as necessary to maintain the required level of service.

23.5.1.3. Identification of Subcontractors (if any).

23.5.2. Contractor Approach: The Contractor's organizational structure detailed within the Resource Management Plan shall coincide with the implementation strategy, and this organizational structure shall determine those named as leads for each work stream across the term of the Contract. Furthermore, the organizational structure shall determine those named in the Resource Management Plan and the biographies required to be included. The Resource Management Plan shall list the location of each named person and their responsible team, and shall describe the Contractor's strategy for interacting with the Department to ensure the Contractor's strategy shall contribute to the successful implementation and operations. The Resource Management Plan shall reference the Contractor's staffing plan. The execution of the staffing plan shall ensure appropriate staffing levels are maintained throughout the term of the Contract and the needs of the Contract are met. Should the Contractor involve one or more Subcontractors during the term of the Contract, those Subcontractors shall be identified

in the Resource Management Plan and shall be subject to providing the same level of detail as the Contractor, including an organizational chart, biographies for key staff, and a description for maintaining appropriate staff levels. As with the Contractor, the Resource Management Plan including Subcontractors shall be reviewed throughout the term of the Contract and shall be updated as necessary.

23.5.3. Deliverable: Resource Management Plan

23.5.4. Deliverable Stage: All Contract Stages

23.6. Reference #2119: Identify and provide resumes for proposed Key Personnel who will be available to perform Work under the Contract.

23.6.1. Any substitutions shall be approved by the Department prior to their assignment to perform Work under the Contract.

23.6.2. Key personnel include:

23.6.2.1. Pharmacy Services Account Manager.

23.6.2.2. Clinical Services Manager.

23.6.2.3. DDI Manager Project.

23.6.2.4. Pharmacy Systems Manager.

23.6.2.5. Pharmacy Call Center Manager.

23.6.2.6. Pharmacist.

23.6.2.7. Rebate Manager.

23.6.3. Other Key Personnel shall be identified by the Contractor, indicating the Contractor's commitment to team stability.

23.6.4. Key Personnel shall be accessible to key Department personnel at all times.

23.6.5. Key Personnel will be evaluated yearly.

23.6.6. All Key personnel shall be dedicated to the Contract and COMMIT project full-time during the term of the Contract.

23.6.7. The Key Personnel required to be located locally are:

23.6.7.1. Pharmacy Services Account Manager.

23.6.7.2. Systems Manager.

23.6.8. Contractor Approach: The Contractor shall identify and provide qualified resumes for the key personnel identified in this Contract. Qualified candidates shall be presented to the Department for approval, and subcontractors, if utilized, shall also be presented to the Department for approval.

23.6.8.1. The Pharmacy Services Account Manager shall be located in the Contractor’s Denver facility and shall be in place by the beginning of the Implementation Phase of the program. This individual shall have experience in leading Medicaid PBMS services and shall excel in the area of project management and scheduling. The Pharmacy Services Account Manager shall provide a single point-of-contact for all

parties involved and researches issues to make informed decisions and shall pull together other resources and meetings to accomplish program goals.

23.6.8.2. The DDI Manager shall also be in place during the Implementation Phase of the program and shall make multiple trips to the Contractor's Denver facility to meet the needs of the Department's Contract deliverables. This individual shall have experience with IT and Operations Project Management with extensive knowledge in managing and leading PBMS solutions.

23.6.8.3. The Pharmacy Systems Manager shall also reside locally in the Contractor's Denver facility and shall be in place by the beginning of the Operations Phase of the program. This role shall center on coordinating system customization and configuration. This individual shall have experience managing the implementation of highly customized enterprise systems and shall work closely with the Pharmacy Services Account Manager to provide superior support to the Department.

23.6.8.4. The Clinical Services Manager shall manage the development of clinical management products and services. The position shall be able to communicate across all departments; have an understanding of the strategic impact of the pharmacy programs for the company, knowledge of how the specialty programs integrate with other clinical initiatives, and expertise with data management. This role shall develop and track the appropriate metrics to monitor the quality of care and the cost impact of the Department's program.

23.6.8.5. The Pharmacy Call Center Manager shall manage the Department's dedicated call center team. This role shall focus on day-to-day performance metrics, developing useful management and client reports, and monitoring individual staff performance and quality scores. This individual shall have experience managing and supervising all phases of the Pharmacy Call Center and Help Desk Services; regularly interacting with Providers and Clients to meet their needs and deliver excellent customer service.

23.6.8.6. The dedicated Pharmacist role shall provide input and feedback on clinical guidelines and discuss patient care with providers and offer alternatives to non-preferred medications. On an as needed basis, the dedicated Pharmacist shall perform clinical reviews for requests outside of clinical guidelines or FDA-approved indications or other requested analysis.

23.6.8.7. All of the above mentioned roles shall be dedicated to the Department program during the term of the Contract and shall be evaluated yearly based on individual and Contract related performance.

23.6.8.8. During the Implementation Phase, the dedicated Contractor Team shall have oversight from the Senior Vice President of Implementations and Account Management. This individual shall provide leadership to the Contractor's Team and travel to the Contractor's facility in Denver on a regular basis for interaction with the Department on all Contract related items.

23.6.8.9. The Contractor's dedicated team members shall also have matrix reporting relationships with Pharmacy Operations, Project Management, and Clinical Pharmacy.

23.6.8.10. There shall also be support staff supporting the Department's program on an allocated basis in order to meet the requirements of the Contract and shall be part of the Resource Management Plan.

23.6.9. Deliverable: Identification and Resumes of Key Personnel

23.6.10. Deliverable Stage: All Contract Stages

23.7. Reference #2120: Key Personnel named shall, at minimum, possess meet the minimum Key Personnel qualifications.

23.7.1. The minimum Key Personnel qualifications are as follows:

23.7.1.1. At least five (5) years of experience in the particular named service (e.g., account management, systems management, pharmacist) preferably within in the health care industry.

23.7.1.2. Demonstrated experience and knowledge of industry standard and best practices regarding large-scale and enterprise-level projects.

23.7.1.3. Specific practical experience their submitted area of expertise.

23.7.1.4. At least three (3) years of experience in performing similar services on complex systems-based modern technology or operational systems.

23.7.1.5. Extensive experience in technical writing.

23.7.1.6. Preferred experience in health care related concepts.

23.7.2. Contractor Approach: For this project, the Contractor shall identify key talent and have a pool of candidates from which to select that shall meet the qualifications contained in this Contract. These resources shall bring knowledge and best practices based on knowledge of other PBMS implementations. There shall also be back-up resources identified during the planning stages for training in the case that any key personnel would leave the program for any unforeseen reason. Recruiting shall begin immediately for the Pharmacy Services Account Manager and the Pharmacy Systems Manager who shall both be located at the Contractor's Denver facility Contractor shall look for similar experienced candidates with PBMS experience that shall meet the qualifications of this Contract. All resumes and potential candidates shall be presented to the Department for approval before appointments or offers are made by the Contractor.

23.7.3. Requirement Stage: All Contract Stages

23.8. Reference #2121: Provide a Pharmacy Services Account Manager for the PBMS Implementation Contract Stage and the PBMS Operations and Enhancements Contract Stage.

23.8.1. The Pharmacy Services Account Manager shall serve as the Contract primary point of contact to maintain communication with the Department's MMIS Contract Administrator and Department Management for activities related to contract administration, project management and scheduling, correspondence between the Department and PBMS Operations, and status reporting to the Department.

23.8.2. The Onsite Pharmacy Services Account Manager shall be in place at the Effective Date and shall reside at the Contractors Denver facility, and be dedicated to the COMMIT project full-time.

23.8.3. Contractor Approach: The Contractor shall provide a qualified Pharmacy Services Account Manager for the PBMS Implementation Contract Stage and the PBMS Operations and Enhancements Contract Stage.

23.8.3.1. The Contractor's Pharmacy Services Account Manager shall be in place by the Effective Date.

23.8.3.2. The Contractor's Pharmacy Services Account Manager shall be dedicated to this Contract as a full-time resource.

23.8.4. Requirement Stage: All Contract Stages

23.9. Reference #2122: Provide a DDI Manager for the PBMS Implementation Contract Stage.

23.9.1. The DDI Manager shall manage activities related to, Contractor resources, Deliverable reviews, system development and testing activities during this Contract Stage. The DDI Manager shall be dedicated to the COMMIT project full-time during this Contract Stage.

23.9.2. The DDI Manager shall be in place at the Effective Date and shall be dedicated to the COMMIT project full-time.

23.9.3. Contractor Approach: The Contractor shall provide a qualified DDI Manager for the PBMS Implementation Contract Stage. The Contractor's DDI Manager shall be in place at the Effective Date and shall be dedicated to this Contract as a full-time resource.

23.9.4. Requirement Stage: PBMS Implementation Contract Stage

23.10. Reference #2123: Provide a Pharmacy Systems Manager for the PBMS Ongoing Operations and Enhancements Contract Stage.

23.10.1. The Pharmacy Systems Manager shall coordinate PBMS Customization and Configuration. The Pharmacy Systems Manager shall be dedicated to the COMMIT project full-time during these Contract Stages.

23.10.2. The Pharmacy Systems Manager shall be in place at the Effective Date and shall reside at the Contractors Denver facility, and be dedicated to the COMMIT project full-time.

23.10.3. Contractor Approach: The Contractor shall provide a qualified Pharmacy Systems Manager for the PBMS Ongoing Operations and Enhancements Contract Stage. The Contractor's Pharmacy Systems Manager shall be in place at the Effective Date and shall be dedicated to this Contract as a full-time resource.

23.10.4. Requirement Stage: PBMS Ongoing Operations and Enhancements Contract Stage

23.11. Reference #2124: Provide a Clinical Services Manager for the PBMS Implementation Contract Stage and the PBMS Operations and Enhancements Contract Stage.

23.11.1. The Clinical Services Manager shall manage all clinical operations activities encompassed in the Contract; overseeing operational and clinical staff; developing operational and clinical policies and procedures.

23.11.2. The Clinical Services Manager shall be in place at the Effective Date and shall be dedicated to the COMMIT project full-time.

23.11.3. Contractor Approach: The Contractor shall provide a Clinical Services Manager for the PBMS Implementation Contract Stage and the PBMS Operations and Enhancements Contract Stage.

23.11.3.1. The Contractor's Clinical Services Manager shall manage all clinical operations activities encompassed in the Contract, oversee operational and clinical staff, and develop operational and clinical policies and procedures.

23.11.3.2. The Contractor's Clinical Services Manager shall be in place at the Effective Date and shall be dedicated to this Contract as a full-time resource.

23.11.4. Requirement Stage: All Contract Stages

23.12. Reference #2125: Provide a Pharmacy Call Center Manager for the PBMS Implementation Contract Stage and the PBMS Operations and Enhancements Contract Stage.

23.12.1. The Pharmacy Call Center Manager shall manage all Call Center operations activities encompassed in the Contract; overseeing Contractor Call Center and Help Desk staff; developing Call Center and Help Desk operational policies and procedures.

23.12.2. The Pharmacy Call Center Manager shall be in place at the Effective Date and shall be dedicated to the COMMIT project full-time.

23.12.3. Contractor Approach: The Contractor shall provide a Pharmacy Call Center Manager for the PBMS Implementation Contract Stage and the PBMS Operations and Enhancements Contract Stage.

23.12.3.1. The Contractor's Pharmacy Call Center Manager shall manage all call center operations activities, oversee Contractor call center and help desk staff, and develop call center and help desk operational policies and procedures.

23.12.3.2. The Contractor's Pharmacy Call Center Manager shall be in place at the Effective Date and shall be dedicated to this Contract as a full-time resource.

23.12.4. Requirement Stage: All Contract Stages

23.13. Reference #2126: Provide a Pharmacist for the PBMS Ongoing Operations and Enhancements Contract Stage.

23.13.1. The Pharmacist shall be the Contractor's clinical lead and be available for escalation issues from the Call Center and Help Desk. The Pharmacist shall also run the Preferred Drug List (PDL).

23.13.2. The Pharmacist shall be in place at the Effective Date and shall be dedicated to the COMMIT project full-time.

23.13.3. Contractor Approach: The Contractor shall provide a Pharmacist for the PBMS Ongoing Operations and Enhancements Contract Stage.

23.13.3.1. The Contractor's dedicated Pharmacist shall be the Contractor's clinical lead and be available for escalation issues from the Call Center and Help Desk. . This individual shall provide input and feedback on clinical guidelines and discuss patient care with providers and offer alternatives to non-preferred medications. The

Pharmacist shall also run the management of the PDL, working in tandem with assigned call center support staff and the Clinical Pharmacist.

23.13.3.2. The Contractor's Pharmacist shall be in place at the Effective Date and shall be dedicated to this Contract as a full-time resource.

23.13.4. Requirement Stage: PBMS Ongoing Operations and Enhancements Contract Stage

23.14. Reference #2126A: Provide a Rebate Manager for the PBMS Implementation Contract Stage and the PBMS Operations and Enhancements Contract Stage.

23.14.1. The Rebate Manager shall manage all aspects of the drug rebate program, including all federal rebates government and supplemental rebates. The Rebate Manager shall also manage all rebates to be collected on encounters.

23.14.2. The Rebate Manager shall be in place at the Contract effective date.

23.14.3. Contractor Approach: Contractor shall provide a Rebate Manager for the PBMS Implementation Contract Stage and the PBMS Operations and Enhancements Contract Stage. Contractor's Rebate Manager shall be the lead on all aspects of the Department's rebate program, including Federal rebates and supplemental rebate programs. This individual shall also be responsible for managing all rebates collected on encounter claims submitted by MCOs. The Rebate Manager shall be in place at the Contract effective date.

23.14.4. Requirement Stage: All Contract Stages

23.15. Reference #2127: Obtain Department review and approval of the Resource Management Plan and materials and any subsequent updates.

23.15.1. The Department will review and approve each update or revision of the Resource Management Plan. Note that the Department's approval of any resource plan does not imply that the staffing levels are sufficient; the Contractor may still have to increase staffing if they are not meeting the Contract requirements.

23.15.2. Contractor Approach: As part of the pharmacy implementation Communication Plan, the Contractor shall establish a schedule for reviewing key processes, approaches, documents and artifacts with the Department for agreement and approval. The Contractor shall leverage the communication processes outlined in the Communication Plan to review and initially obtain approval for the Resource Management Plan. Subsequent reviews to The Resource Management Plan shall also be reviewed with the Department following an agreed upon approach. These reviews shall occur throughout the implementation and within each of its 12 phases.

23.15.3. Requirement Stage: All Contract Stages

23.16. Reference #2128: Provide sufficient staff to perform Work for System development, operations and maintenance, claims/ encounters processing, and Call Center and Help Desk services, as defined in this Contract.

23.16.1. The Contractor shall increase staffing levels if requirements or standards are not being met at no additional cost to the Department.

23.16.2. Contractor Approach: The Contractor shall maintain a staffing plan throughout the pharmacy implementation and its 12 phases. The pharmacy Staffing Plan shall be reviewed, updated and approved as outlined in the Project Management Plan and Resource Management Plan. The Contractor shall leverage these reviews to assess performance across the pharmacy implementation to ensure it has sufficient staff to perform the work required to meet the obligations of the Contract. The Contractor shall review its staffing to validate it has qualified staff in place throughout the implementation. The Contractor shall ensure its staffing is appropriate to meet the needs of the Contract across system development, operations and maintenance, claims / encounters processing, call center and help desk, and any additional areas agreed upon by the Contractor and the Department. If the standards of the Contract are not being met as per the Project Management Plan and the Resource Management Plan, the Contractor shall make modifications to its Staffing Plan to ensure the standards of the Contract are met at no additional cost to the Department

23.16.3. Requirement Stage: All Contract Stages

23.17. Reference #2129: Provide sufficient staffing resources to support architecture and design activities to ensure that the PBMS and supporting technical and business activities relying on the PBMS are not interrupted.

23.17.1. The Contractor shall increase staffing levels if requirements or standards are not being met at no additional cost to the Department.

23.17.2. Contractor Approach: Through the use of a continuous Resource Management Plan that is evaluated throughout the life of the Contract, the Contractor shall ensure sufficient staffing resources to support architecture and design activities to ensure that the PBMS project and supporting technical and business activities relying on the PBMS are not interrupted.

23.17.2.1. The Resource Management Plan shall be submitted to the Department for approval.

23.17.2.2. The Contractor shall increase staffing levels if requirements or standards are not met at no additional cost to the Department.

23.17.3. Requirement Stage: PBMS Ongoing Operations and Enhancements Contract Stage

23.18. Reference #2130: Provide the personnel and resources necessary for the automated and/ or manual sampling of claims/ encounters and reference file data, including, but not limited to, the retrieval of historical data for auditing, quality control, and research.

23.18.1. The Contractor shall increase staffing levels if requirements or standards are not being met at no additional cost to the Department.

23.18.2. Contractor Approach: The Contractor shall provide the personnel and resources necessary for the automated and/or manual sampling of claims/encounters and reference file data, including but not limited to, the retrieval of historical data for auditing, quality control, and research.

23.18.2.1. The Contractor shall increase staffing levels if requirements or standards are not being met, at no additional cost to the Department.

23.18.3. Requirement Stage: All Contract Stages

23.19. Reference #2131: Support the Department in all testing activities by providing support staff, technical expertise and the tools required to track activities, outcomes, and test results.

23.19.1. Contractor Approach: Testing activities shall continue through the term of the Contract and shall have varied levels through the different phases. The Contractor shall provide the personnel and resources necessary to support the Department in all testing activities by providing support staff, technical expertise and the tools required to track activities, outcomes, and test results. This shall be an interactive process with collaboration between the Contractor and the Department, and testing resources shall be increased during periods of significant testing within the defined Enhancement Hours.

23.19.2. Requirement Stage: All Contract Stages

23.20. Reference #2132: Provide the Department the ability to conduct an exit interview with PBMS Staff who resign or the Department shall receive an exit questionnaire completed by the resigning employee.

23.20.1. Contractor Approach: In the case of a staff resignation, the Contractor's Human Resources team shall conduct an exit interview.

23.20.1.1. The Contractor shall make available to the Department the results of the interview in the form of a questionnaire completed by either the resigning employee or by the interviewer. The Contractor shall follow up, fully investigate any issues, and report findings to the Department.

23.20.2. Requirement Stage: All Contract Stages

23.21. Reference #2133: Use of Subcontractors shall be clearly explained in the Resource Management Plan, and any Subcontractor shall be identified by the organization's name.

23.21.1. At a minimum, the Subcontractor information shall include all of the following:

23.21.1.1. Name of each Subcontractor.

23.21.1.2. Address of each Subcontractor.

23.21.1.3. The general scope of work to be performed by each Subcontractor.

23.21.1.4. Each Subcontractor's willingness to perform such work.

23.21.1.5. A Certification from each Subcontractor that it does not discriminate in its employment practices.

23.21.2. The Contractor shall report to the Department annually any information on its use of Subcontractors, certifying that the Subcontractor meets the employment practices mandated by federal and State of Colorado statutes and regulations.

23.21.3. In the event that the Contractor hires a new subcontractor within the annual time frame, the Contractor shall notify the Department within thirty (30) Business Days of the hiring process of the new Subcontractor.

23.21.4. Contractor Approach: The Contractor expects it shall perform all PBMS requirements as specified in this Contract without the need to hire subcontractors. In the event that The Contractor hires a new subcontractor within the annual time frame, the Contractor shall notify the Department within 30 days and serve as the single point of contact for

all services the subcontractor performs. Subcontractors shall be thoroughly evaluated in terms of ability to perform the desired work and ensuring that they do not discriminate in any employment practices. The Contractor shall collaborate with the Department and verify that all Subcontractors meet the employment practices mandated by federal and State of Colorado statues and regulations.

23.21.5. Requirement Stage: All Contract Stages

23.22. Reference #2134: The Contractor shall manage and be accountable for the actions, inactions, and performance of all Subcontractors. The Contractor is solely responsible for the Work performed under this Contract including the work of Subcontractors. The Contractor is the Department's single point of contact for all services to be performed under this Contract including services performed by Subcontractors.

23.22.1. Contractor Approach: The Contractor expects it shall perform all PBMS requirements as specified without the need to hire Subcontractors.

23.22.1.1. In the event that the Contractor elects to engage or utilize a Subcontractor, the Contractor understands that they are solely responsible for all work performed by Subcontractors. The Contractor shall manage and be accountable for the actions, inactions, and performance of all Subcontractors. The Contractor shall be solely responsible for the Work performed under this Contract including the work of Subcontractors.

23.22.1.2. In the event that the Contractor elects to engage or utilize a subcontractor to complete the work on the PBMS Project, the Contractor shall be the single point of contact for all services performed under this Contract.

23.22.2. Requirement Stage: All Contract Stages

23.23. Reference #2135: The Contractor shall manage all aspects of the Contract that affect price, schedule, performance (scope and quality), risk/ issues/ opportunities, and applicable resources. The Contractor shall provide transparency into its management plans and execution. The Department expects an approach such that "if the Contractor sees it, the Department sees it" to minimize asymmetric understanding of the Contract status.

23.23.1. Contractor Approach: The Contractor shall provide transparency throughout the term of the Contract and identify potential issues surrounding price, risk/issues/opportunities, and applicable resources. The Contractor's DDI Manager shall leverage the Project Management Plan for Time and Schedule Management and follow the PMI and PMBOK standard processes in this knowledge area. The schedule shall allow ample time for project team members to complete all tasks.

23.23.1.1. Each Milestone task shall be staffed with the appropriate resources. The Contractor shall manage schedule risks by having proper staff assigned to tasks at the right time.

23.23.1.2. Status progress shall be communicated as often as needed, in accordance with the Communication Management Plan, as it relates to critical path and key milestones on the schedule.

23.23.1.3. The Contractor shall use proven best practice PMI tools and techniques to ensure they develop the schedule with accurately estimated activities and timelines. This approach shall include:

23.23.1.3.1. Developing an activity list along with key milestones

23.23.1.3.2. Leveraging network diagrams to plan activities

23.23.1.3.3. Developing a resource breakdown structure

23.23.1.3.4. Estimating the duration of individual activities

23.23.1.3.5. Developing the project schedule

23.23.1.3.6. The use of stage gates to ensure on time, satisfactory completion of SDLC phases

23.23.1.3.7. Measuring performance and change requests,

23.23.1.4. Further, each DDI Project Manager in the Contractor's organization shall be cross-trained to manage project implementations, IT infrastructure projects and other special projects. In the unlikely event the DDI Project Manager is out of the office, another Project Manager shall manage the project. The result shall be that no time will be lost on the project and that the Department shall always have a focal point at the Contractor.

23.23.1.5. The Contractor shall review the project schedule with the Department, including the user acceptance testing section, before the start of the project. The Contractor shall develop a risk management plan and risk register that shall, at a minimum, contain: description of the risk, description of the impact to the project, an impact scoring method, a probability of occurrence, description of the mitigation plan, dates and times associated, priorities, etc. Risk management plans shall continuously be updated throughout the project. Risk Management may include, but is not limited to:

23.23.1.5.1. Understanding and clarifying the request for changes to the project and analyzing the impact of each change to the cost and schedule

23.23.1.5.2. Analyzing a change of direction, timelines, deliverables, etc., and the impact of each to the project

23.23.1.5.3. Keeping track of all the different Change Requests that have been received that may be a risk for the project and the status of each

23.23.1.5.4. Deciding whether to accept the change and incorporate the revised definitions into the project plan or reject the change and continue with the current plan

23.23.1.5.5. Communicating with the project team the risk associated with each issue or change.

23.23.2. Requirement Stage: All Contract Stages

24. PROJECT MANAGEMENT AND REPORTING

24.1. Reference #2136: The Contractor shall develop, support, report (using Dashboards), and provide weekly project management reports on the status of the project activities to allow

both the Contractor and the Department to assess the progress for the PBMS during the Project Phases.

24.1.1. Contractor Approach: The Contractor shall provide the Department with status reports during all Project Phases, as described in the Communication Management Plan. These reports shall be prepared by the DDI Project Manager during the implementation phase and by the Pharmacy Services Account Manager during operations. The report shall be submitted to the Department by uploading it to the shared document repository. From there it shall be accessible to authorized Department users and subject to the deliverable submission, review and approval process as described in the Communication Management Plan.

24.1.2. Deliverable: Weekly Project Management Reports

24.1.3. Deliverable Stage: All Contract Stages

24.2. Reference #2137: The Contractor shall provide reporting on all aspects of the Contract that affect price, schedule, performance (scope and quality), risk/ issues/ opportunities, and applicable resources, as defined by the Communication Management Plan.

24.2.1. Contractor Approach: The Contractor's Project Management Organization shall have an collection of tools that enable the project management resources to effectively define, monitor, and report status on various project management components, including budget, schedule, resource utilization, milestones, deliverables, issues, and changes.

24.2.1.1. The Contractor shall maintain a full library of standardized Project Management Plan document templates that shall be available to the team and cover all Project Phases.

24.2.1.2. The Contractor shall utilize finely tuned processes based on industry best practices to facilitate, track, and control project artifacts. The Contractor shall incorporate the use of these tools and techniques in the administration of the PBMS implementation.

24.2.1.3. The Contractor shall utilize a document repository to store implementation artifacts, key project documentation, and other information deemed important to the PBMS Project or is requested of by the Department. The implementation portal shall be available 24 hours a day, seven days a week and requires login credentials to view posted content. A resource documentation log shall also be available to describe each document and to identify when it was created, revised, and approved by the Department.

24.2.2. Deliverable: Price, Schedule, Performance, Risk/Issues/Opportunities and Resource Reporting

24.2.3. Deliverable Stage: All Contract Stages

24.3. Reference #2138: The Communication Plan shall include a monthly Contract Management Report.

24.3.1. The monthly Contract Management Report shall include the following:

24.3.1.1. Progress toward achieving goals stated in the business plan.

24.3.1.2. Activities, by each function or unit of the Contractor organization (e.g., claims/ encounters, Provider Enrollment and Relations).

24.3.1.3. Achievement of performance standards for the previous month and identification of all performance standards that were not met.

24.3.1.4. A summary of Contractor activities and key volume indicators, for the month and cumulative to the fiscal year end.

24.3.1.5. Establish the Quarterly Milestones and reporting schedule.

24.3.1.6. Establish the Dispute Process trigger mechanism (to submit an item for resolution via the dispute process via letter, email, and phone).

24.3.1.7. Other activities necessary for the Department to monitor Contractor activities.

24.3.2. Monthly reports shall be provided to the Department within seven (7) Business Days following the close of the month the report covers.

24.3.3. Contractor Approach: The Contractor's Pharmacy Services Account Manager and DDI Project Manager shall develop a Monthly Contract Management Report as part of the broader Communication Plan. This report shall be an update and status on critical program elements and shall be reviewed with key Department personnel on a monthly basis. The report shall be delivered to the Department within seven Business Days following the close of the month the report covers and shall include all agreed upon activities and metrics to be reviewed. The template shall be designed at the beginning of project initiation based on collaboration between the Contractor and the Department. All of the critical elements defined in the Contract and requested by the Department shall be documented and reviewed in a regularly scheduled project meeting. The report and the review shall drive follow-up actions where necessary and set program priorities and direction for the following month where the status of each item or corrective action where needed shall again be reviewed. The Contractor shall use the Contractor's shared document repository for storage of the Monthly Contract Management Report so all key Contractor and Department personnel can view the reports for project updates and follow-up.

24.3.4. Deliverable: Monthly Contract Management Report

24.3.5. Deliverable Stage: All Contract Stages

24.4. Reference #2139: Participate in weekly status meetings in person or by telephone/ video conference call, as approved by the Department, to review status reports. The Contractor shall be responsible for providing the meeting space and conference line/ virtual meeting place for the Department and the Contractor.

24.4.1. Contractor Approach: The Contractor's DDI Project Manager and Account Manager shall facilitate weekly status meetings in an agreed upon meeting space or by teleconference/virtual meeting place for the Contractor and Department throughout the PBMS implementation. The DDI Project Manager and Account Manager shall solicit meeting topics from all members of the project team, including the Department, and shall provide an agenda prior to each meeting occurrence. The Contractor shall present the current project status dashboard, and shall cover milestones recently achieved and milestones to be accomplished over the next reporting period. The DDI Project

Manager and Account Manager shall also facilitate conversation around issues and challenges, and shall discuss any actionable plan when necessary. The Contractor's project status reporting shall include an update on the overall health of the project and a discussion of issues or risks that may affect schedule, budget, or deliverables during each phase of the project. The DDI Project Manager and Account Manager shall track action items and provide meeting minutes within 24-hours of the meeting end. Furthermore, the DDI Project Manager and Account Manager shall ensure actionable items are assigned, tracked and fulfilled prior to the next status meeting. The Contractor shall provide the meeting space and conference line/virtual meeting place.

24.4.2. Requirement Stage: All Contract Stages

24.5. Reference #2140: Ensure that the Contractor's staff attending applicable meetings between the Department and the Contractor have the authority to represent and commit the Contractor regarding work planning, problem resolution, and program development.

24.5.1. Contractor Approach: The Contractor's DDI Project Manager and Pharmacy Services Account Manager, or their designee attending meetings with the Department, shall have the authority to represent and commit the Contractor regarding work planning, problem resolution, and program development. Based on the Contractor's flexible reporting structure and access to support staff and executive team members, quick escalation of unforeseen issues or needed approvals shall occur. In the event that the Contractor requires different people to provide approvals during a meeting, the Contractor shall ensure that those people are present at that meeting.

24.5.2. Requirement Stage: All Contract Stages

24.6. Reference #2141: Provide all necessary software to support Transmittals and the process the Contractor and Department will use to submit, review, and approve Transmittals.

24.6.1. The Contractor shall provide all necessary software to support all electronic communications involved in day-to-day activities associated with the Contract.

24.6.2. Contractor Approach: The Contractor shall provide a shared document repository into which all project deliverables shall be uploaded. The repository will require web access and a standard web browser in order for authorized users to access the repository. The Contractor shall configure the shared document repository to allow users to submit, review and approve Transmittals.

24.6.3. Requirement Stage: All Contract Stages

24.7. Reference #2142: Enable all assigned Contractor personnel to easily exchange documents and electronic files with the Department in compatible formats.

24.7.1. The Contractor shall maintain the same software and version of software as the Department including, but not limited to, the following:

24.7.1.1. Microsoft Word.

24.7.1.2. Microsoft Excel.

24.7.1.3. Microsoft Project.

24.7.1.4. Microsoft Access.

24.7.1.5. Microsoft PowerPoint.

24.7.2. The Contractor shall upgrade within thirty (30) Business Days of the Department's notification of upgrade.

24.7.3. Contractor Approach: The Contractor shall maintain compatible desktop applications with the Department for exchanging documents. The standard desktop installations for the Department shall include: Microsoft Word, Microsoft Excel, Microsoft Access, Microsoft PowerPoint, and Microsoft Project. The Contractor shall review the current desktop standard of the Department and ensure document compatibility.

24.7.3.1. Upon notification of a Microsoft version change at the Department level, the Contractor shall have 30 days to upgrade its desktop environments, in accordance with the Contractor's corporate standards, used to exchange documents with the Department to meet the new standard.

24.7.4. Requirement Stage: All Contract Stages

24.8. Reference #2143: Stay abreast of pharmacy related federal and State initiatives and work in partnership with the Department to identify possible solutions and resolutions to meet the changing requirements. The Contractor shall participate in National Medicaid EDI Healthcare Workgroup (NMEH) and National Council for Prescription Drug Program (NCPDP) groups and national list serves.

24.8.1. Contractor Approach: The Contractor shall participate in NMEH and NCPDP groups and national list servs. The Contractor shall coordinate activities to inform the Department of new regulatory compliance mandates, including modified HIPAA Final Rule mandates. The Contractor shall work closely with and participate in the NCPDP workgroups, Workgroups for Electronic Data Interchange (WEDI), NMEH, CMS, and other regulatory groups to ensure that the Department is aware of Regulatory Compliance initiatives. The Contractor shall translate key initiatives or policies that impact the Department and shall work directly with the Pharmacy Services Account Manager to communicate possible solutions and resolutions to meet changing requirements.

24.8.2. Requirement Stage: All Contract Stages

24.9. Reference #2144: Notify the Department immediately of any potential PBMS problems and the potential impact of those problems, including unscheduled downtime.

24.9.1. The Contractor shall report any problems within 30 minutes of Contractor identifying problem and shall notify appropriate Department staff by phone and email, as outlined in Communication Management Plan.

24.9.2. Contractor Approach: The Contractor shall immediately notify the Department as specified in the Communication Management Plan to communicate any potential or realized PBMS problems including infrastructure and unscheduled downtime.

24.9.3. Requirement Stage: All Contract Stages

24.10. Reference #2145: Provide reconciliation reporting on all claims/ encounters processes.

24.10.1. This includes reconciliation of data that is transferred from PBMS to MMIS.

24.10.2. Contractor Approach: The Contractor shall provide reconciliation reporting to ensure that all claims and encounters transferred between the PBMS and MMIS are accounted for.

24.10.3. Deliverable: Reconciliation Reporting on all Claims/Encounters

24.10.4. Deliverable Stage: All Contract Stages

24.11. Reference #2146: Perform the research to identify impacts and root causes of PBMS problems, and communicate to the Department a plan to resolve problems. Implement the plan to resolve problems and report the results to the Department.

24.11.1. Contractor Approach: The Contractor shall incorporate a systematic ongoing quality management process into day-to-day operations. This process shall include organizational and administrative activities in support of process improvement planning, organization, and measurement. The continuous process improvement components shall include, but are not limited to root cause analysis and reporting.

24.11.1.1. After achieving the resolution of a PBMS incident, the Contractor's Pharmacy Services Account Manager and Operations Manager shall collaborate with appropriate corporate resources to identify the impacts and root cause. The resolution shall be documented as the recommended resolution to the problem through the issue management process and corrective action plans where needed and delivered to the Department. Based on recommendation, it may be necessary to document a change request and obtain approval through the change control process. Once the Department approves the resolution approach, the team shall implement the resolution, and then the Contractor’s Quality Assurance staff shall monitor the process to ensure executed improvement initiatives produce the results expected.

24.11.2. Requirement Stage: All Contract Stages

24.12. Reference #2147: The Contractor’s project management software shall be compatible with the Department's project management software.

24.12.1. Contractor Approach: The Contractor shall use Microsoft Project as project management software which is compatible with Clarity. Updates to project work plans may be exchanged through the Contractor's shared document repository.

24.12.2. Requirement Stage: All Contract Stages

24.13. Reference #2148: Capture and collect notification of undeliverable communication (e.g., return receipt notice from email, or undeliverable notice from mail) and update address information as appropriate.

24.13.1. Contractor Approach: The Contractor shall capture and collect all return receipt and undeliverable notices and update address information as appropriate and as directed by the Department. The Contractor shall work with the Department, as described in the Communication Management Plan, to remove invalid contact information and correct the contact information.

24.13.2. Requirement Stage: PBMS Ongoing Operations and Enhancements Stages

24.14. Reference #2149: Contractor shall provide weekly reports that include metrics on interactions used for communications by the Contractor with clients and providers.

24.14.1. Contractor Approach: The Contractor shall update stakeholders on progress of the project, performance achievements, client and provider interaction metrics, and key volume statistics on a weekly basis. The reports shall be distributed both electronically and delivered to the Department to be made available via web portal. The Contractor shall collaborate with the Department to define the individual reporting requirements, documentation and delivery style, naming conventions, and distribution lists. All metrics reports shall adhere to the Deliverable submission, review, and approval process as described and approved by the Department within the Communication Management Plan.

24.14.2. Deliverable: Weekly Client and Provider Interaction Report

24.14.3. Deliverable Stage: All Contract Stages

24.15. Reference #2150: Provide an efficient and effective PBMS reporting process.

24.15.1. This includes, but is not limited to:

24.15.1.1. Incorporate Department comments and revisions.

24.15.1.2. If a Deliverable is rejected, Contractor shall work with the Department to determine review schedule.

24.15.1.3. If a Deliverable is rejected, the Department will determine the changes the Contractor shall perform before it will be reviewed again.

24.15.1.4. Support report balancing and verification procedures.

24.15.1.5. Maintain comprehensive list of standard reports and their intended use.

24.15.1.6. Maintain online access to at least four (4) years of selected management reports.

24.15.2. Contractor Approach: The Contractor shall utilize a shared document repository that shall allow secure access to authorized personnel. With appropriate access, users shall be able to store documents including Department comments and revisions. The Contractor shall provide a process, supported by the shared document repository, by which deliverable artifacts shall be delivered to the Department for review. If the deliverable is rejected, the Contractor shall perform the changes identified by the Department in the deliverable prior to re-submission of the deliverable to the Department for additional review. The Contractor shall provide a similar process for the submission of reports which shall include support for report balancing and verification. The Contractor shall maintain a comprehensive inventory of standard reports along with their intended use. The Contractor shall utilize a shared document repository to maintain online access to at least four (4) years of selected management reports.

24.15.3. Requirement Stage: PBMS Implementation Contract Stage

24.16. Reference #2151: Assist in developing processing forms and instructions to be used internally with Department staff.

24.16.1. Contractor Approach: The Contractor shall support the Department in the development of processing forms and instructions to be used with internal Department personnel as well as forms and instructions for external stakeholders use.

24.16.2. Requirement Stage: All Contract Stages

25. CONTRACTOR RESPONSIBILITIES

25.1. Reference #2152: Provide price and schedule estimates to support proposed legislation, budget requests, and other initiatives, as directed by the Department.

25.1.1. After receiving notification and requirements from the Department, Contractor will respond within two (2) Business Days during the Colorado Legislative Session, within five (5) Business Days outside of the Colorado Legislative Session, or as agreed to by the Department through the Change Management Plan.

25.1.2. Contractor Approach: The Contractor's dedicated Colorado Pharmacy Services Account Manager shall collaborate with internal support resources to provide the Department price and schedule estimates to support proposed legislation, budget requests, and other initiatives, as directed by the Department.

25.1.2.1. After receiving notification and requirements from the Department, Contractor shall respond within two (2) Business Days during the Colorado Legislative Session, within five (5) Business Days outside of the Colorado Legislative Session, or as agreed to by the Department through the Change Management Plan.

25.1.3. Deliverable: Price and Schedule Estimates

25.1.4. Deliverable Stage: All Contract Stages

25.2. Reference #2153: Develop and maintain a process to provide assistance (technical and business process related) as needed to assist users in researching problems, reviewing production outputs and understanding report formats.

25.2.1. Contractor Approach: The Contractor's Account Manager shall be the first line of contact for the Department users who need support in researching problems, reviewing production outputs, and understanding report formats. The Contractor's Account Manager shall be responsible for identifying the Department needs, and engaging other Contractor subject matter experts (SMEs) to work directly with Department users to provide training, direction, or assistance needed in using the Contractor's systems or reports. The Department users shall be provided full training on each system needed to perform their research or other functions, as well as training on the PBMS reporting tools. The Contractor's Training department shall also provide user guides and job aides to Department users in the use of the Contractor's systems and reporting tools. These user materials shall be updated as business processes and systems change. During the DDI process, the Contractor shall identify Department user functions, and develop a Training Plan based on those needs. Once operational, the Account Manager shall ensure the Department users are connected directly with the needed Contractor SMEs to provide any assistance needed in researching problems, or performing their daily functions in using the Contractor's systems and reports.

25.2.2. Requirement Stage: All Contract Stages

25.3. Reference #2154: Coordinate with other contractors that provide batch control, balancing and scheduling of data load cycles (e.g., eligibility files, financial payment processing).

25.3.1. Contractor Approach: The Contractor shall interact and coordinate with other contractors as deemed necessary by the Department through the Contractor's established data interface process that provides batch control, balancing and scheduling of data load cycles including eligibility files and financial payment processing. The Contractor shall have the required capability and experience working with trading partners such as external data and solution providers, including those that provide drug pricing, third party liability solutions, program integrity offerings, and Drug Utilization Review services.

25.3.1.1. The Contractor shall produce reports, where appropriate, that shall be used for balancing and there shall be controls in place to measure the data quality before loading the data. The Contractor shall apply interface best practices which include batch controls that have header, trailer and data content and the contents shall be validated against the header and trailer records. The Contractor shall schedule interfaces using the TIDAL scheduler and automatic monitoring. All of the above mentioned interfaces shall be scheduled and they shall be monitored 24 hours a day, 7 days a week, and 365 days a year by an operational team.

25.3.1.2. The Contractor shall have communication and data exchange protocols in place with CMS, First Databank (FDB), and NCPDP as well as a variety of other organizations who work to provide data in support of Pharmacy Benefit programs across the nation as directed by the Department.

25.3.2. Requirement Stage: All Contract Stages

25.4. Reference #2155: Identify and track all errors and discrepancies found in the PBMS, notify the Department, and correct all errors and discrepancies.

25.4.1. Contractor Approach: The Contractor shall follow a tracking and oversight process in order to provide visibility into actual progress so that management can take effective actions when performance deviates from plan. All the errors and discrepancies shall be tracked using defect identification and problem resolution tracking tool as determined by the Department. The Contractor shall notify the Department of all errors and discrepancies it identifies.

25.4.2. Requirement Stage: All Contract Stages

25.5. Reference #2156: Support the Department and its contractor(s) in Independent Verification and Validation (IV&V) activities associated with the Contract.

25.5.1. Contractor Approach: The Contractor shall support the Department and its contractors in IV&V activities associated with the Contract.

25.5.2. Requirement Stage: PBMS Implementation Contract Stage

25.6. Reference #2157: Purchase and maintain infrastructure hardware and software updates including upgrades and technology refreshes to maintain functionality of all interfaces.

25.6.1. Contractor Approach: The Contractor shall procure the hardware and software needed for a successful operations and maintenance throughout the term of the Contract. The

Contractor shall review and maintain current technology to maintain functionality of all supported interfaces. The Contractor shall manage the associated, maintenance and licensing agreements for the purchases made. The Contractor shall maintain current technology including the proper execution of system upgrades, database upgrades, critical patch update for software and server and infrastructure technology refreshes.

25.6.2. Requirement Stage: All Contract Stages

25.7. Reference #2158: Manage and maintain software upgrades and site licenses so they are compatible with standard Department software. Provide training on software upgrades authorized System users, as necessary.

25.7.1. Contractor Approach: The Contractor shall review, manage and maintain software upgrades so they remain compatible with standard Department software. The Contractor shall manage the associated, maintenance and site licensing agreements for software used in the delivery of the PBMS. The Contractor shall be responsible for the successful implementation of all software upgrades and for ensuring that proper installation and deployment instructions are followed and coordinated with the Department. The software installation shall adhere to the Deliverable submission, review, and approval process as described and approved by the Department within the Change Management Plan. The Contractor shall develop and deliver training associated with software upgrades.

25.7.2. Requirement Stage: All Contract Stages

25.8. Reference #2159: Adhere to the Deliverable submission, review, and approval process as described and approved by the Department within the Change Management Plan.

25.8.1. Contractor Approach: The Contractor shall follow the submission, review and approval process contained in the Change Management Plan.

25.8.2. Requirement Stage: All Contract Stages

25.9. Reference #2160: Perform Statement on Standards for Attestation Engagements No. 16 (SSAE-16) audits annually (by an independent auditor) at the PBMS facility and data center sites. Responses to findings, action plans, and remediation plans shall be submitted to and approved by the Department. Coordinate responses to initial findings with the Department that may impact Department operations.

25.9.1. Contractor Approach: The Contractor shall annually provide the results of an SSAE-16 Audit to the Department.

25.9.1.1. The SSAE-16 Audit shall be performed by a reputable auditing firm and in compliance with the standard SOC1 SSAE16, previously known as SAS70 standard.

25.9.1.2. Action and remediation plans shall be submitted to and will be subject to approval by the Department.

25.9.1.3. Submission, review, and approval as necessary shall be described in and will be approved by the Department within the Communication Management Plan.

25.9.2. Deliverable: Annual SSAE-16 Audit

25.9.3. Deliverable Stage: All Contract Stages

25.10. Reference #2161: Provide reasonable access to and the ability to inspect, all facilities (or any site) in which the Contractor or Subcontractor(s) performs any Work related to this Contract or maintains any records related to this Contract and provide assistance to the federal and State representatives during audits, inspections and evaluations.

25.10.1. Contractor Approach: The Contractor shall grant access and the ability to inspect to individuals within the company or at the Department, ensuring that access to the Contractor's facilities, records, and documents are readily available for inspection by personnel with the appropriate security clearance. The Contractor shall also provide assistance to the federal and Department representatives during audits, inspections, and evaluations.

25.10.2. Requirement Stage: All Contract Stages

25.11. Reference #2162: Contractor will have insight into internal policy discussions, contractual issues, price negotiations, State financial information, and advanced knowledge of potential/ draft legislation. As a result, the Contractor shall maintain confidentiality and privacy of this information.

25.11.1. Contractor Approach: The Contractor's Security and Privacy Plan shall ensure completeness and coverage to maintain confidentiality and privacy of this information.

25.11.2. Requirement Stage: All Contract Stages

25.12. Reference #2163: Contractor shall work cooperatively with all Department staff, State staff, and other contractors to ensure success of this Contract. In addition, the Contractor shall identify efficiencies for the Department that could be leveraged by altering requirements, changing functionality, adapting business processes, or making other changes to the architecture or overall solution.

25.12.1. Contractor Approach: The Contractor's dedicated key personnel and support resources shall identify efficiencies for the Department that could be leveraged by altering requirements, changing functionality, adapting business processes or making changes to the architecture or overall solution. The Contractor shall recommend changes based on a flexible and configurable technology platform and structured change management process. Recommendations shall be discussed with the Department and defined within the Contractor change management process. Levels of Effort and any needed Statement of Work (SOW) shall be defined with the Department and agreed upon before the Contractor makes any changes to PBMS and Services functionality.

25.12.2. Requirement Stage: All Contact Stages

25.13. Reference #2164: Ensure that all PBMS data, related to claims, encounters, and authorized processing, is delivered to the MMIS and/or BIDM, as directed by the Department, in order to support reporting and analysis by the BIDM. This data includes prior authorization data, including clinical notes.

25.13.1. Contractor Approach: The Contractor shall ensure that all PBMS data, related to claims, encounters, and authorized processing, is delivered to the MMIS and/or BIDM, as directed by the Department, to support reporting and analysis by the BIDM. All interfaces shall be scheduled and monitored by Contractor and the Contractor shall

clearly document trouble shooting procedures. If the Department directs the Contractor to provide the same data to more than one recipient or if the file layout to transmit the same data to more than one recipient is different between recipients, and the requirement to transmit the data to the recipient or to modify the file layout is not already provided through a requirement in Exhibit A, the Contractor may use the Dispute Process, as described in §20.E to discuss the increased resources required. For this section, examples of recipients would be the MMIS and BIDM.

25.13.2. Requirement Stage: PBMS Ongoing Operations and Enhancements Contract Stage

25.14. Reference #2165: On an annual basis, prepare a Business Plan for Department review and approval. Department staff will participate in initial planning activities.

25.14.1. The Business Plan shall be a working long-term document that describes how potential changes to technology (e.g., Near Field Communication) and/ or architecture could improve operations.

25.14.2. The Business Plan will be reviewed and approved by the Department and shall be revised by the Contractor, as necessary, to reflect changing situations throughout the year. The Business Plan shall include:

25.14.2.1. An outline of all major activities and training planned for the upcoming year.

25.14.2.2. Business improvement objectives for the upcoming year.

25.14.2.3. Methodology for performing activities and meeting objectives.

25.14.2.4. Recommendations in any area the Contractor feels improvements can be made, based on industry standards, best practices and/ or cost efficiencies.

25.14.2.5. Plan for coordinating with and interfacing with the MMIS and BIDM contractors to meet operational responsibilities.

25.14.2.6. Plan for coordinating with and interfacing with the MMIS and BIDM contractors to meet operational responsibilities.

25.14.3. The Business Plan shall be delivered to the Department for approval during the Operations and Maintenance Phase and then annually updated thirty (30) Business Days prior to the beginning of each State fiscal year.

25.14.4. The Contractor shall prepare a six- (6-) month evaluation of activities performed as compared to the Business Plan, and revise the Business Plan, as necessary, to reflect updated goals and activities.

25.14.5. Contractor Approach: Working with the Department, the Contractor shall develop an annual Business Plan that shall outline Contractor's plan to deploy systems and services over the coming year. Contractor's development of the annual Business Plan shall be supported by inputs from one or more subsidiary management plans and other planning documents, including scope management, time management, and cost management. The annual Business Plan is a living document provided to the Department during the Operations and Maintenance Phase and then annually updated thirty (30) Business Days prior to the beginning of each State fiscal year. The Business Plan shall include:

25.14.5.1. An outline of all major activities and training planned for the upcoming year

25.14.5.2. Business improvement objectives for the upcoming year

25.14.5.3. Methodology for performing activities and meeting objectives

25.14.5.4. Recommendations in any area the Contractor feels improvements can be made, based on industry standards, best practices and/ or cost efficiencies

25.14.5.5. Plan for coordinating with and interfacing with the MMIS and BIDM contractors to meet operational responsibilities

25.14.5.6. A six month evaluation of activities performed as compared to the Business Plan, and revise the Plan as necessary to reflect updated goals and activities.

25.14.6. Deliverable: Annual Business Plan

25.14.7. Deliverable Stage: PBMS Ongoing Operations and Maintenance Contract Stage

25.15. Reference #2166: Ensure that all Systems data from the PBMS are delivered to the BIDM and/or MMIS in order to support reporting and analysis.

25.15.1. The Contractor shall provide daily updates except as otherwise recommended by the Contractor and accepted by the Department.

25.15.2. Contractor Approach: The Contractor shall ensure that all PBMS data, related to claims, encounters, and authorized processing, is delivered to the MMIS as directed by the Department to support reporting and analysis and to the BIDM as directed by the Department.

25.15.3. Requirement Stage: PBMS Ongoing Operations and Enhancements Contract Stage

25.16. Reference #2167: THIS REQUIREMENT INTENTIONALLY DELETED

25.17. Reference #2168: THIS REQUIREMENT INTENTIONALLY DELETED

25.18. Reference #2169: Maximize use of industry standards for PBMS design and exchange of data.

25.18.1. Contractor Approach: The Contractor shall comply with all HIPAA Transaction and Code Set standards for the electronic processing of covered transactions and commits to maintaining compliance with HIPAA, industry standards, and customer data quality standards throughout the term of the Contract. The Contractor shall implement these standards in coordination with a schedule agreed to with the MMIS and/or BIDM vendors, as directed by the Department, and the State for interfaces applicable to the provision of PBMS services.

25.18.1.1. Contractor shall support Electronic Data Interface (EDI), File Transfer Protocol (FTP), and SOAP/XML, with FTP with PGP encryption as Contractor's preferred process for transmitting and receiving files.

25.18.1.2. Contractor shall support the use of industry standard data exchange using industry leading tools, including Oracle Fusion, EDIFECS, and Informatica. These tools shall run on high performance AIX, Linux, and Windows servers that provide load-balancing, parallel processing, and concurrent file processing of all HIPAA transactions. The Contractor shall develop and test all HIPAA-compliant transactions (including the components for COB), and receive and send 837P, 837I, 820, 835, 834, 270, 271, 276, and 277 transactions, in addition to the 278.

25.18.1.3. The Contractor shall use the TA1 and 999 standard responses and the 5010 versions of the 277 unsolicited transactions as an additional host-load notice for 837 claims feeds. The fully functional HIPAA validator shall provide WEDI level-1 through level-6 validations, as well as level-7 companion guide edits.

25.18.1.4. Supported Industry Standard Data Exchange Standards shall include:

25.18.1.4.1. HIPAA transaction sets for 5010

25.18.1.4.2. 270/271/271U/276/277/277U/278/820/834/835/837

25.18.1.4.3. professional, institutional, dental/999

25.18.1.4.4. 270/271/835/834 for Pharmacy accounts

25.18.1.4.5. NCPDP Transactions D.0 and batch 1.2:

25.18.1.4.5.1. B1/B2/B3

25.18.1.4.6. Post Adjudication 2.2/3.0

25.18.1.4.7. Health Level 7 Transactions – Coordination of Care Documents (CCD).

25.18.1.5. The Contractor shall update supported industry standards as those standards change throughout the term of the Contract.

25.18.2. Requirement Stage: All Contract Stages

25.19. Reference #2170: Provide audit support to the Department, including selection of samples, production of hard-copy documents, and gathering of other required data. The Contractor shall assist Department staff in responding to all federal and State auditing agencies. This level of support shall also be provided to all other State and federal audit agencies or their designees.

25.19.1. Contractor Approach: The Contractor shall provide audit support to the Department, including selection of samples, production of hard copy documents, and gathering other required data. Processes shall be in place to sample data access and update activity. The Contractor shall assist the Department staff in responding to all federal and State auditing agencies as well as supporting the auditing staff of these agencies.

25.19.2. Requirement Stage: All Contract Stages

26. DELIVERABLE REQUIREMENTS

26.1. Reference #2171: Report on PBMS project progress and status in writing no less than weekly. The use of real-time Dashboard presentations is preferred to allow key metrics to be available in near real time. Weekly reports shall include the status of schedule, performance (quality/ scope/ technical/ operations), risks/ issues/ opportunities, staffing, and other pertinent metrics. The Contractor shall be responsible for preparing and distributing meeting minutes for Department review, and maintaining final approved agenda/ minutes.

26.1.1. Agenda and status report shall be delivered 24 hours prior to the meeting.

26.1.2. Minutes shall be distributed no later than close of business on the third Business Day following the meeting.

26.1.3. Contractor Approach: The Contractor shall provide weekly reports on project status and updates through regularly scheduled operational meetings. Agendas and updated reports shall be sent to all key personnel at least twenty-four (24) hours prior to the meeting and Contractor shall provide meeting minutes and follow-up within three (3) Business Days. Contractor shall work with the Department to support and provide assistance to determine which key metrics it would like available in a dashboard format.

26.1.3.1. The Contractor shall provide a report in a dash board format which contains a variety of metrics agreed upon by Contractor and The Department. The Pharmacy Services Account Manager shall facilitate these weekly meetings to review the relevant topics with key Contractor and Department personnel. The Pharmacy Services Account Manager shall work with the appropriate IT resources, reporting personnel and data base administrators to obtain and report the key data elements. This data shall support the Department in both managing its program as well as monitoring service level agreement levels. Other types of information shall be able to be be updated on a monthly basis. On a monthly basis the Contractor's FirstRx data base area shall provide an array of reports which detail metrics such as plan covered lives, hours of system availability, maintenance window downtime totals, adjudication response time/ claims adjudication totals in one-half (0.5) second intervals and average adjudication time.

26.1.3.2. During the Ongoing Operations and Enhancement Contract Stage, the Contractor's reporting team shall produce a monthly accounts payable (A/P) report which provides the numbers of paid claims, voided claims and denied claims along with the corresponding payment amounts for each claim type. This report also shall provide the number of enrolled recipients, the number of utilizing members and the number of dual eligible recipients. Other agreed upon metrics shall be able to be added along with the aforementioned report information into a concise dash board report for the Department.

26.1.4. Deliverable: Weekly System Project Progress Report; System Progress Meeting Minutes

26.1.5. Deliverable Stage: All Contract Stages

26.2. Reference #2172: The Contractor shall develop, in accordance with the Project Management Institute's standards contained in the Project Management Book of Knowledge (PMBOK), a Change Management Plan.

26.2.1. The Change Management Plan shall address and define processes for managing changes to the project such as:

26.2.1.1. Establish a process to manage Change Requests.

26.2.1.2. Changes in the scope of work.

26.2.1.3. Changes in business process definition.

26.2.1.4. Changes in federal or State regulatory change support.

26.2.1.5. Changes to the budget and procurement activities.

26.2.1.6. Changes in Configuration and Customization (i.e., Configuration Management as defined in industry terms).

26.2.1.7. Schedule for routine PBMS maintenance and upgrading PBMS software.

26.2.1.8. Changes in training needs.

26.2.2. This Deliverable shall be completed and provided to the Department during the Initiation and Planning Phase.

26.2.3. Contractor Approach: The Contractor shall establish a structured Change Request Advisory Board with Department and Contractor representatives.

26.2.3.1. The Contractor shall create a structured method to facilitate change requests and approvals following PMBOK industry standards.

26.2.4. Deliverable: Change Management Plan

26.2.5. Deliverable Stage: All Contract Stages

26.3. Reference #2173: The Contractor shall obtain Department review and approval of the Change Management Plan and materials and any subsequent updates prior to use. The Change Management Plan shall be implemented once approved and the Contractor shall adhere to the processes included in the plan.

26.3.1. Contractor Approach: The Contractor's Change Management Process shall include Contractor review and Department approval of all modifications to the Change Management Plan.

26.3.2. Requirement Stage: All Contract Stages

26.4. Reference #2174: Meet with the Department weekly on the status of all active System Enhancements or projects as defined in the Change Management Plan.

26.4.1. Contractor Approach: Contractor shall facilitate weekly project status meetings with the Department Project Team comprised of Department staff and key leads from Contractor, who are responsible for implementation and operation of each system and operational component of the program. Weekly meetings shall focus on status of system enhancements as well as key deliverables and associated tasks, planned activity for the week, open issues and action items associated with outstanding deliverables, and risks and mitigation plans.

26.4.2. Requirement Stage: All Contract Stages

26.5. Reference #2175: As defined in the Change Management Plan, develop, maintain, and submit for Department approval all SDLC documentation, including all requirements, test planning, technical specifications, User Acceptance Testing (UAT), test results, post-implementation verifications, data conversion, strategy, and System documentation.

26.5.1. Contractor Approach: The Contractor shall deliver to the Department for approval artifacts of the implementation and operations which shall include documents describing requirements, test planning, technical specifications, user acceptance test results, readiness review results, data conversion details, and system administration. These documents shall be uploaded by the Contractor into a shared document repository so that authorized Department users may view all documentation. The

shared document repository shall also facilitate the agreed upon deliverable approval process.

26.5.2. Deliverable: SDLC Documentation

26.5.3. Deliverable Stage: All Contract Stages

26.6. Reference #2176: Deliverables shall meet the Department-approved standards, format and content requirements, and the Department will specify the number of copies and type of media for each Deliverable.

26.6.1. Contractor Approach: The Contractor shall submit documentation deliverables that shall meet the Department approved standards which shall be fully documented by the Department prior to the delivery of the first deliverable by the Contractor. The documentation provided by the Department to the Contractor shall specify the number of copies, type of media and other standards. The Contractor's implementation manager shall oversee the Contractor's compliance with the agreed-upon attributes of each deliverable.

26.6.2. Requirement Stage: All Contract Stages

27. TRAINING

27.1. Reference #2177: Provide training and support for providers on the Health Insurance Portability and Accountability Act (HIPAA) and HIPAA compliance for all transactions involving the PBMS.

27.1.1. Contractor Approach: The Contractor shall provide training to pharmacy providers to review HIPAA and HIPAA compliant transactions for all claims and billing procedures involving the PBMS.

27.1.2. Requirement Stage: All Contract Stages

27.2. Reference #2178: Propose, develop, produce, publish and deliver HIPAA compliant training materials specific to the System for the Department and its designees.

27.2.1. Contractor Approach: The Contractor shall provide HIPAA compliant training materials, manuals, and job aids. The materials shall include detailed procedural steps, field descriptions, and glossaries. Training materials shall be derived from scrubbed or ummy data that resides in the training environment of the PBMS so any use of PHI is eliminated.

27.2.2. Deliverable: HIPAA Training Materials

27.2.3. Deliverable Stage: All Contract Stages

27.3. Reference #2179: Coordinate the roll out, delivery, publication and distribution of all PBMS training programs and PBMS training materials across all functional areas.

27.3.1. Contractor Approach: The Contractor shall coordinate the roll out, delivery, publication, and distribution of all PBMS training programs and training materials across all functional areas. The details shall be captured in the Contractor’s Pharmacy Training Plan.

27.3.2. Requirement Stage: All Contract Stages

27.4. Reference #2180: As defined in Training Plan, provide support, including, but not limited to, on-site training or video conferencing if required, to instruct providers in using the billing application or to facilitate the resolution of billing problems.

27.4.1. Contractor Approach: The Contractor shall provide on-site or web-based training to instruct providers on claims billing procedures and inquiry systems. All questions shall be recorded and the information shall be disseminated to trainees in the form of a Frequently Asked Questions (FAQ) document.

27.4.2. Requirement Stage: All Contract Stages

27.5. Reference #2181: Develop and deliver a comprehensive training program to support the roll out of the System.

27.5.1. This training shall be provided to both Department staff and Contractor staff.

27.5.2. Contractor Approach: The Contractor shall develop and deliver a comprehensive training program to support the roll out of the PBMS by completing a detailed needs analysis with Department stakeholders and SMEs to determine which courses are required and the appropriate audiences and timing.

27.5.3. Requirement Stage: PBMS Implementation Contract Stage

27.6. Reference #2182: As part of organizational readiness preparation, schedule and conduct interviews and sessions with the Department's subject matter experts (SMEs) and stakeholders, as required, to clarify the training and readiness expectations and requirements.

27.6.1. Contractor Approach: The Contractor shall complete the needs analysis in Reference #2181 during the Operational Readiness Phase. The Contractor shall schedule and conduct interviews and sessions with the Department’s SMEs and stakeholders to complete this analysis.

27.6.2. Requirement Stage: PBMS Implementation Contract Stage

27.7. Reference #2183: As part of testing and in conjunction with organizational readiness conduct structured acceptance testing training for the Department and its designees per the Training Plan.

27.7.1. Contractor Approach: The Contractor shall conduct User Acceptance Testing (UAT) training for the Department and its designees prior to the start of the UAT phase. A training agenda shall be provided and shall include tailored training materials to meet the needs set forth by the Department.

27.7.2. Requirement Stage: PBMS Implementation Contract Stage

27.8. Reference #2184: Maintain ongoing training programs for Contractor staff and Department staff in the use of the reference functions.

27.8.1. This training shall occur at least annually.

27.8.2. Contractor Approach: The Contractor shall provide training on any new initiatives, as needed, throughout the life of the Contract. These training courses shall be offered as instructor-led, Web based, or computer-based trainings (CBTs) as agreed upon by the Department. The Contractor shall deliver a comprehensive training program to support

the rollout of the PBMS applications. Reference functions shall include how a user will use online help as well as find and use PBMS reference files.

27.8.3. Requirement Stage: All Contract Stages

27.9. Reference #2185: THIS REQUIREMENT INTENTIONALLY DELETED

27.10. Reference #2186: Provide the ability for video conferencing (or other remote method) training participation and presentations.

27.10.1. Contractor Approach: The Contractor shall provide the ability for web-based training participation and presentations.

27.10.2. Requirement Stage: All Contract Stages

27.11. Reference #2187: As defined in the Training Plan, train Department and Contractor staff as well as other authorized PBMS users on the PBMS billing procedures and current Colorado medical assistance pharmacy programs policy in inquiry response processes. Provide training evaluation reports by participant or summaries of evaluations to the Department.

27.11.1. Contractor Approach: The Contractor shall provide training to Department and Contractor staff on the PBMS billing procedures and current Colorado medical assistance pharmacy programs policy in inquiry response processes. To track attendance, the Contractor shall require students to complete course sign-in sheets and/or register online and complete course evaluation forms.

27.11.2. Deliverable: Training Evaluation Reports

27.11.3. Deliverable Stage: All Contract Stages

27.12. Reference #2188: THIS REQUIREMENT INTENTIONALLY DELETED

27.13. Reference #2189: Provide training on any new PBMS initiatives that occur through the term of the Contract.

27.13.1. This training shall be provided to both Department staff and Contractor staff.

27.13.2. Contractor Approach: The Contractor shall provide training on any new PBMS initiatives, as needed, throughout the term of the Contract. These training courses shall be offered as instructor-led, Web-based, or computer-based trainings (CBTs) as agreed upon by the Department.

27.13.3. Requirement Stage: All Contract Stages

27.14. Reference #2190: THIS REQUIREMENT INTENTIONALLY DELETED

27.15. Reference #2191: Track and provide confirmation of attendance at all training sessions and what versions of training materials were presented at the training.

27.15.1. Contractor Approach: The Contractor shall track attendance at all training sessions by the use of sign in sheets and/or online course registration. All training manuals shall include a revision history by date as part of the standard template.

27.15.2. Requirement Stage: All Contract Stages

28. SECURITY AND CONFIDENTIALITY REQUIREMENTS

28.1. Reference #2192: Comply with federal and State security criteria as outlined by the Colorado Office of Information Security, Office of Civil Rights, etc. in the standard system security plan template.

28.1.1. Contractor Approach: The Contractor shall meet all state and federal privacy and security regulatory requirements, including those with the HIPAA Security Rule and HITECH Act and those outlined criteria as outlined by the Colorado Office of Information Security, Office of Civil Rights.

28.1.1.1. The Contractor shall demonstrate via routine vulnerability assessments and technology security audits a multi-layered approach to monitor for system vulnerabilities whether they are to theft, mischief, tampering, or even non-malicious factors such as natural disasters.

28.1.2. Requirement Stage: All Contract Stages

28.2. Reference #2193: Provide detailed security control implementation and status information.

28.2.1. The security control implementation and status information shall include the following Control Categories:

28.2.1.1. Management Controls:

28.2.1.1.1. Risk Assessment.

28.2.1.1.2. Planning.

28.2.1.1.3. Systems and Services Acquisition.

28.2.1.1.4. Certification, Accreditation and Security.

28.2.1.1.5. Program Management.

28.2.1.2. Operational Controls:

28.2.1.2.1. Personnel Security.

28.2.1.2.2. Physical and Environmental Protection.

28.2.1.2.3. Contingency Planning.

28.2.1.2.4. Configuration Management.

28.2.1.2.5. Maintenance.

28.2.1.2.6. PBMS and Information Integrity.

28.2.1.2.7. Media Protection, Incident Response.

28.2.1.2.8. Security Awareness and Training.

28.2.1.3. Technical Controls:

28.2.1.3.1. Identification and Authentication.

28.2.1.3.2. Access Controls.

28.2.1.3.3. Audit and Accountability.

28.2.1.3.4. PBMS and Communications Protection.

28.2.2. Contractor Approach: The Contractor shall provide a Physical and System Security Plan that is based on International System Security Certification Consortium (ISC2) — the international standard for IT security — and the National Institute of Standards and Technology (NIST). The plan shall include all technical, physical, and administrative safeguards to enhance physical security, personnel security, and information systems security. The plan shall demonstrate the Contractor's compliance with the HIPAA Standards for Privacy, Electronic Transactions and Security.

28.2.2.1. The Physical and System Security Plan shall serve as the mechanism for providing detailed security control implementations and status information (where applicable) for the following Control Categories:

28.2.2.1.1. Management Controls: Risk Assessment, Planning, Systems and Services Acquisition, Certification, Accreditation and Security, and Program Management.

28.2.2.1.2. Operational Controls: Personnel Security, Physical and Environmental Protection, Contingency Planning, Configuration Management, Maintenance, PBMS and Information Integrity, Media Protection, Incident Response, and Security Awareness and Training.

28.2.2.1.3. Technical Controls: Identification and Authentication, Access Controls, Audit and Accountability, and PBMS and Communications Protection.

28.2.3. Requirement Stage: All Contract Stages

28.3. Reference #2194: Demonstrate that the PBMS infrastructure (hardware, software, and linkages) is operational and meets federal and State architectural, technical, security and privacy requirements as well as the business and functional requirements. Architectural, technical, security and privacy requirements shall be defined as all requirements of Exhibit H and the MECT requirements.

28.3.1. Contractor Approach: The Contractor shall provide a system certification and volume stress test document that demonstrates to the Department that the PBMS infrastructure (hardware, software, and linkages) is operational and meets all applicable Federal and State architectural, technical, security and privacy requirements as well as the business and functional requirements prior to "Go Live". The document shall detail the system architecture, hardware and software configurations, the PBMS infrastructure tests performed, expected test results, and actual results of a volume load test.

28.3.2. Requirement Stage: All Contract Stages

28.4. Reference #2195: Keep all documents, data compilations, reports, computer programs, photographs, and any other work provided to or produced by the Contractor in the performance of the Contract confidential until publicly released by the Department or until written permission is granted by the Department for its release.

28.4.1. Contractor Approach: The Contractor shall keep confidential all documents, data compilations, reports, computer programs, photographs and other work provided to or produced by the Contractor in the performance of the Contract. The Contractor shall continue to keep all of the aforementioned artifacts confidential until publicly released by the Department or until written permission is granted by the Department for its

release. The Contractor shall store all such artifacts on only secure systems so that access shall be controlled to only designated Contractor and Department resources based on their job role.

28.4.2. Requirement Stage: All Contract Stages

28.5. Reference #2196: Obtain written approval from the Department prior to disclosing any privileged information (e.g., attorney/ client information).

28.5.1. Contractor Approach: The Contractor shall not disclose any privileged information, such as attorney-client, member information, or other information classified as privileged, without obtaining prior approval from the Department, unless required by law. The Contractor shall ensure requests fall within the Department's specified guidelines for requesting disclosure and the policy shall be documented in appropriate personnel documentation/training material for Colorado personnel. This shall include but is not limited to HIPAA training.

28.5.1.1. The Contractor shall acknowledge its understanding of the Department's Address Confidentiality Program (ACP) and the guidelines regarding disclosure of member and provider information related to the program. The Contractor's Communication Management Plan shall detail the program guidelines for maintenance and release of information for members covered under this policy. The Contractor shall safeguard personal health information per HIPAA regulations for ACP members.

28.5.2. Requirement Stage: All Contract Stages

28.6. Reference #2197: Provide the ability for any user, as defined by the Department, to have secure, role-based, Single Sign-On user access to any current and historical data, PBMS components, or Web-based material.

28.6.1. Contractor Approach: The Contractor shall deploy a secure, role-based, Single Sign On (SSO) process for granting user access to current or historical data within the PBMS systems and Web based applications. A valid federation trust shall be setup between the Contractor and Department for the purpose of accomplishing SSO capabilities between the entities. The Contractor shall standardize on Security Assertion Markup Language (SAML) 2.0 and shall collaborate with the Department to determine the application roles needed to ensure the proper exchange of SAML assertions.

28.6.2. Requirement Stage: All Contract Stages

28.7. Reference #2198: Provide client and provider information protection per Colorado's Address Confidentiality Program (ACP) as specified through the Communication Management Plan.

28.7.1. Contractor Approach: The Contractor shall maintain protection of information in the ACP as specified in the Communication Management Plan.

28.7.2. Requirement Stage: All Contract Stages

28.8. Reference #2199: Provide a third party cyber security assessment to execute the security audit prior to go-live. The selected third party assessor will work with the Colorado Office of Information Security and provide reports to the Department.

28.8.1. Contractor Approach: The Contractor shall coordinate and execute a third party cyber security assessment and vulnerability test prior to go-live. The Contractor and its third party assessor shall work with the Colorado Office of Information Security to define the level of reports that are acceptable to disclose based on the sensitive nature of the data. The Contractor shall mitigate any issues or risks found during the assessment within the agreed upon timeframe defined during the assessment review with the Colorado Office of Information Security.

28.8.2. Requirement Stage: PBMS Implementation Contract Stage

28.9. Reference #2200: Apply all security patches for any Windows Operating System and any other software for the PBMS.

28.9.1. Contractor shall inform Department that patches are available within twenty-four (24) hours of receipt of the patches. Contractor shall coordinate with the Department for deployment.

28.9.2. Contractor Approach: The Contractor shall review the Microsoft Security Responses released via Microsoft Security Bulletins and determine the urgency of vulnerabilities and related software updates once released. A patch evaluation process shall be initiated and documented prior to the release of any Windows Operating System patch deployment.

28.9.2.1. The Contractor shall inform the Department that patches are available within 24 hours of receipt to coordinate an appropriate deployment schedule. The Contractor shall properly install all service packs, revisions and patches are and ensure that proper installation instructions are followed and coordinated with the Department.

28.9.3. Requirement Stage: All Contract Stages

28.10. Reference #2201: Provide a user administration module that allows authorized System users, including authorized providers and System administrators, to assign access to System functions in a secure manner in accordance with privacy and security requirements.

28.10.1. Contractor Approach: External access to the Contractor's systems shall be governed by role-based security just like internal users. In addition to traditional role based security, providers shall only be granted access to claims submitted by them or their provider group. Group membership shall be delegated to the provider organization itself and controlled through User Access Control (UAC), a web based application.

28.10.2. Requirement Stage: All Contract Stages

28.11. Reference #2202: THIS REQUIREMENT INTENTIONALLY DELETED

28.12. Reference #2203: Provide privacy/ litigation controls that indicate who/ what have access to provider data contained within the provider/ client record.

28.12.1. Contractor Approach: The Contractor shall provide controls that identify and limit user accounts granted access to all data, including provider data, within the PBMS. These controls shall include but are not limited to the following

28.12.1.1. All information shall be held under the control of a logical access control system that is approved by the Contractor's Chief Security Officer in partnership/collaboration with the Identity Provider (IdP)

28.12.1.2. Unique User ID and password shall be required for computer-connected network access

28.12.1.3. Incorrect login information shall not be disclosed in partnership/collaboration with the IdP.

28.12.1.4. System login banner displays security rules for access in partnership/collaboration with the IdP.

28.12.1.5. Notice of last login time and date shall be recorded for security review

28.12.1.6. Multiple simultaneous online sessions shall be prohibited

28.12.1.7. User IDs shall uniquely identify a single user in partnership/collaboration with the IdP.

28.12.1.8. Periodic review and reauthorization of user access privileges shall be required in partnership/collaboration with the IdP.

28.12.1.9. Signed forms shall be required for issuance of User IDs in partnership/collaboration with the IdP.

28.12.1.10. User profiles shall identify system access allowed by job role

28.12.1.11. Default User IDs shall be disabled, removed, or amended from the default state.

28.12.1.12. The Contractor shall enforce standard naming conventions in partnership/collaboration with the IdP.

28.12.1.13. The Contractor shall control all applications used on the Contractor's systems in partnership/collaboration with the IdP.

28.12.1.14. The Contractor shall provide dedicated account administration in partnership/collaboration with the IdP.

28.12.1.15. All of the Contractor's systems and applications shall comply with the HCA Information Technology Security Policy requirements in partnership/collaboration with the IdP.

28.12.2. Requirement Stage: All Contract Stages

28.13. Reference #2204: Provide the ability to support both role-based and group-based security at the individual data field level so that users are not able to view sensitive information or other information which they have no business need to view.

28.13.1. This includes suppressing the results returned from searches as well as information viewable in the user's own display environment.

28.13.2. Contractor Approach: The PBMS shall provide role-based and group-based security. This shall control access to data by defining at the individual data field level what can be made accessible through the application's graphical user interface on a role or group basis.

28.13.3. Requirement Stage: All Contract Stages

28.14. Reference #2205: Provide the ability for security personnel to view, in real time, the exact same screens and information being viewed by an authorized PBMS user.

28.14.1. Contractor Approach: The Contractor's security team shall maintain the ability to shadow user sessions in real-time. The security application used shall display the exact screen information being viewed by an authorized PBMS user.

28.14.2. Requirement Stage: All Contract Stages

29. AUDIT REQUIREMENTS

29.1. Reference #2206: Provide the ability to review all changes made to fields in the PBMS and maintain an audit trail for all actions performed.

29.1.1. Contractor Approach: The Contractor shall provide the ability to review all changes made to fields, including both changes to the fields themselves as well as to information contained in the fields, to maintain an audit trail for all actions performed.

29.1.2. Requirement Stage: All Contract Stages

29.2. Reference #2207: THIS REQUIREMENT INTENTIONALLY DELETED

29.3. Reference #2208: Maintain audit trail of all actions performed on a client record.

29.3.1. This includes:

29.3.1.1. Eligibility, ineligibility and retro eligibility, and associated spans.

29.3.1.2. Enrollment/ Disenrollment spans and benefit package enrollment, limitations and changes.

29.3.1.3. Communication and notification activities.

29.3.1.4. Sources of eligibility.

29.3.1.5. Provide cross-reference of prior client ID's.

29.3.2. Contractor Approach: The Contractor shall ensure that user update and timestamp activity logic exists for all actions performed on the client records.

29.3.2.1. The Contractor's application audit trail shall exist for additions, updates and deletes for:

29.3.2.1.1. Eligibility, ineligibility and retro eligibility, and associated spans.

29.3.2.1.2. Enrollment/ Disenrollment spans and benefit package enrollment, limitations and changes.

29.3.2.1.3. Communication and notification activities.

29.3.2.1.4. Sources of eligibility.

29.3.2.1.5. Provide cross-reference of prior client ID's.

29.3.2.2. These access trails shall be retained in the application database and be retrievable through the application user access points.

29.3.2.3. The Contractor shall provide reporting detail pertaining to the database audit trails upon request from the Department or other investigative analysis teams.

29.3.3. Requirement Stage: All Contract Stages

29.4. Reference #2209: Maintain an audit trail for each claim record (e.g., each stage of processing, the date of each stage of claim processing, and any error codes posted).

29.4.1. Contractor Approach: The Contractor shall ensure that for each claim record an audit log that records each stage of processing, the date of each stage of claim processing, and any error codes posted are maintained. The claim audit trails shall be retained in the application database and be retrievable through the application user access points.

29.4.2. Requirement Stage: All Contract Stages

29.5. Reference #2210: Provide the ability to quickly and easily track the life cycle of claims/ encounters from original submission date through all adjustments, including partial and PBMS-generated adjustments.

29.5.1. Contractor Approach: The PBMS shall contain audit trail functionality that allows an authorized user to easily track the life cycle of claims and encounter data including but not limited to the original submission and all adjustments.

29.5.2. Requirement Stage: All Contract Stages

29.6. Reference #2211: THIS REQUIREMENT INTENTIONALLY DELETED

29.7. Reference #2212: Maintain an audit trail of all actions performed and any data modifications initiated from the interface feed.

29.7.1. Contractor Approach: The PBMS shall contain audit trail functionality that shall maintain a history of actions performed by interfaces.

29.7.2. Requirement Stage: All Contract Stages

29.8. Reference #2213: Ensure that all audit trails are easy-to-use (e.g., through the use graphical User Interfaces, paper layouts) easy to read (e.g., little or no use of codes or abbreviations) and easy to understand (e.g., activities and logs use complete English sentences describing what happened).

29.8.1. Contractor Approach: The PBMS shall contain audit trail functionality that allows an authorized user to view the history of activity for an item. This information shall be displayed through a graphical user interface of the PBMS, be easy to read with little use of codes and easy to understand for any user with knowledge of the pharmacy business process.

29.8.2. Requirement Stage: All Contract Stages

29.9. Reference #2214: THIS REQUIREMENT INTENTIONALLY DELETED

29.10. Reference #2215: Support the logging, tracking, and auditing of web access for any client-data or provider-data queries.

29.10.1. Contractor Approach: The Contractor shall keep records of all Web Based PBMS application access rights granted and terminated throughout the term of the Contract. In addition, the Contractor shall log all access/viewing of client data PHI/PII.

29.10.1.1. The audit trails shall include the following information:

29.10.1.1.1. A unique log-on or terminal ID, the date, and time of any create/modify/delete action and, if applicable, the ID of the system job that effected the action

29.10.1.1.2. The date and identification “stamp” displayed on any on-line inquiry

29.10.1.1.3. The client information viewed/Accessed.

29.10.1.2. The Contractor shall provide reporting detail pertaining to the PBMS applications and access rights upon request from the Department or other investigative analysis teams. This data shall be stored in commercial auditing tools or custom, application logs that store the fields returned and query statement used to retrieve the data.

29.10.2. Requirement Stage: All Contract Stages

29.11. Reference #2216: Maintain screens which allow users the ability to view and print the entire audit trail in the PBMS.

29.11.1. Contractor Approach: The Contractor shall ensure that user update and timestamp activity logic exists for the PBMS. These access trails shall be retained in the application database and the entire audit trail shall be viewable and retrievable through the PBMS application user access points. For auditing activities related to system and database level access the Contractor shall maintain an interactive screen access point to the audit reporting tool which shall allow designated users the ability to view and print the entire audit trail.

29.11.2. Requirement Stage: All Contract Stages

30. COMPLIANCE WITH FEDERAL STANDARDS

30.1. Reference #2217: The PBMS shall meet the federal requirements for certification and licensure as prescribed in the State Medicaid Manual, Part 11, as well as 42 and 45 CFR.

30.1.1. Contractor Approach: The PBMS and Services shall comply with all applicable state and federal requirements, including any related to CMS certification. The Contractor shall constantly review statutes, regulations and CMS policy to validate that systems and business processes comply. In addition, regular audits shall be performed by external entities and all findings shall be addressed.

30.1.2. Requirement Stage: All Contract Stages

30.2. Reference #2218: Maintain and make available source data and methodological documentation from all federal reports for the purposes of validating and verifying data and report information. Ensure data is transferred correctly to the PBMS.

30.2.1. Contractor Approach: The Contractor shall maintain source data from which reports are derived for the purpose of subsequent validation and verification. Any change shall contain a date time stamp and the ID of the user or process responsible for the change. This architecture shall allow the Contractor to know the state of any record at any time.

30.2.2. Requirement Stage: All Contract Stages

30.3. Reference #2219: Provide client and provider communications that meet the health literacy levels established by the federal (National Institute for Health) and State guidelines.

30.3.1. Contractor Approach: The Contractor shall collaborate with the Department on all client and provider communications to ensure that the communications meet the health literacy levels established by the federal (National Institute for Health) and state

guidelines. All communications shall have Department reviews and approvals prior to distribution.

30.3.2. Requirement Stage: All Contract Stages

30.4. Reference #2220: Provide published content that meets 6th grade reading literacy levels on client facing materials.

30.4.1. Contractor Approach: Contractor shall collaborate with the Department on all published client facing materials to ensure the content meets the 6th grade reading literacy levels. All materials shall have Department reviews and approvals prior to distribution.

30.4.2. Requirement Stage: All Contract Stages

31. DISASTER RECOVERY AND BUSINESS CONTINUITY

31.1. Reference #2221: Provide results of Business Continuity and Disaster Recovery Plan testing. Allow Department Staff or their designee to participate in testing, if requested by the staff.

31.1.1. Business Continuity and Disaster Recovery Plan testing shall occur at least annually.

31.1.2. Contractor Approach: DR-BCCP rehearsals shall be completed at least annually for the PBMS by Contractor staff and shall allow for participation from Department staff. Rehearsal results shall be summarized and reported to the Department within three week of exercise completion. The recovery teams shall keep detailed logs for use in updating their failover, activations plans, backup, and recovery procedures at the conclusion of each exercise. Activation plans and recovery plans shall be reviewed quarterly and updated at the end of each exercise or as changes in the Contractor's datacenter environment dictate.

31.1.3. Requirement Stage: All Contract Stages

32. DATA RETENTION

32.1. Reference #2222: Maintain current and historical client claims and encounters pricing and utilization data, and transfer to MMIS in accordance with the PBMS Operations and Maintenance Plan.

32.1.1. Contractor Approach: The Contractor shall maintain current and historical client claims/ encounters pricing and utilization data, and transfer to MMIS and/or BIDM, in accordance with the Operations and Maintenance Plan.

32.1.2. The Contractor shall maintain a master index of all records maintained pursuant to its records retention responsibilities that shall, for each record, include the name, span of dates covered, and volume and medium.

32.1.3. The Contractor shall define the data retention periods in accordance with direction by the Department.

32.1.4. Requirement Stage: PBMS Ongoing Operations and Enhancement Stage

32.2. Reference #2223: Maintain all current and historical provider (electronic and paper) and client (electronic) records in accordance with the PBMS Operations and Maintenance Plan.

32.2.1. Contractor Approach: The Contractor shall maintain all current and historical provider and client records in accordance with the PBMS Operations and Maintenance Plan.

32.2.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Stage

32.3. Reference #2224: Keep records, as specified by the Department, involving matters in litigation, for the period of time agreed upon in accordance with the PBMS Operations and Maintenance Plan.

32.3.1. Contractor Approach: The Contractor shall keep records involving matters in litigation for the period of time agreed upon with the Department. The Contractor shall store paper records at least until a verified electronic copy of the document exists. Electronic records shall be maintained for the term of the Contract.

32.3.2. Requirement Stage: All Contract Stages

32.4. Reference #2225: Maintain a current and updated cross-walk between National Drug Code (NDC) and Health Care Common Procedure Code (HCPCS)/Common Procedure Code (CPT), and maintain historical cross-walk data for claims/ encounters processing and drug rebate in accordance with the PBMS Operations and Maintenance Plan.

32.4.1. The Contractor shall update this cross-walk at least once every calendar quarter.

32.4.2. Contractor Approach: The Contractor shall maintain a current and updated cross-walk between NDC and HCPCS/ CPT, and maintain historical cross-walk data for claims/encounters processing and drug rebate under purview of this Contract as needed and requested by the Department. Retention of these records shall comply with all the PBMS Operations and Maintenance plan.

32.4.3. Deliverable: Updated NDC-HCPCS/CPT cross-walk

32.4.4. Deliverable Stage: All Contract Stages

32.5. Reference #2226: Retain all original paper submitted by providers under the Contract until quality, human readable electronic media is produced of that material in accordance with the PBMS Operations and Maintenance Plan.

32.5.1. Contractor Approach: The Contractor shall retain all original paper submitted by providers until there is a quality, human readable electronic analog produced. The Contractor shall put in place processes that record the verification of the image so that it is available to trace the origin of the paper document.

32.5.2. Requirement Stage: All Contract Stages

32.6. Reference #2227: Contractor shall ensure that data maintained by the PBMS are properly and routinely purged, archived, and protected from destruction, as appropriate, as identified in the Operations Procedures Plan in accordance with the PBMS Operations and Maintenance Plan.

32.6.1. Contractor Approach: The Contractor shall purge, archive and protect from destruction all data maintained by the PBMS as identified in the Operations Procedures Plan. The Contractor shall perform regular backups of all PBMS data and routinely move the backups off-site to preserve it in the event of a catastrophic failure at the data center. The Contractor shall have the ability to purge data from its systems, but shall not

routinely do so to allow historical data to be accessible to the PBMS for the term of the Contract.

32.6.2. Requirement Stage: All Contract Stages

32.7. Reference #2228: The Contractor shall retain and archive electronic media specified by the Operations Procedures Plan in accordance with the PBMS Operations and Maintenance Plan.

32.7.1. Contractor Approach: The Contractor shall retain and archive electronic media specified by the Operations Procedures Plan. The Contractor shall perform regular backups of all PBMS data and routinely move the backups off-site to preserve it in the event of a catastrophic failure at the data center. The Contractor shall have the ability to purge data from its systems, but shall not routinely do so to allowing historical data to be accessible to the PBMS for the term of the Contract.

32.7.2. Requirement Stage: All Contract Stages

32.8. Reference #2229: Data retention for Protected Health Information shall comply with HIPAA Privacy Standards, and data generated and/ or maintained by the PBMS shall be retained and be accessible according to federal and State Requirements.

32.8.1. Contractor Approach: The Contractor shall comply with the standards set by the Department for all types of records. Data retention for PHI shall comply with HIPAA Privacy Standards, and data generated and/ or maintained by the PBMS shall be retained and be accessible according to federal and State Requirements.

32.8.2. The Contractor shall ensure all data retention requirements are met throughout the term of the Contract and during system sun-setting activities and any type of Contract close out activities. The Contractor shall fulfill the regulatory and statutory standards as they apply to the Technical Infrastructure and the Systems and Services, and Shared Services computing environments. The Contractor's System Engineering Management Plan shall include a full list of standards and regulations pertaining to records retention of which the Contractor maintains compliance.

32.8.3. Requirement Stage: All Contract Stages

32.9. Reference #2230: Provide ability to archive and index the archived data with the ability to access a directory view of the archive's contents.

32.9.1. When data is requested from the archive, the request will be addressed within five (5) Business Days, and the request will be fulfilled within thirty (30) Business Days.

32.9.2. Contractor Approach: The Contractor shall maintain the capability to archive and index the archived data. The Contractor shall provide the ability to access a directory view of the archive's contents. When data is requested from the archive, the request shall be addressed within five (5) Business Days, and the request shall be fulfilled within thirty (30) Business Days.

32.9.3. Requirement Stage: All Contract Stages

32.10. Reference #2231: Provide a data storage archive and management approach that allows a "never delete a record" approach for ease and timeliness in accessing historical records, if so chosen by the Department.

32.10.1. Contractor Approach: The Contractor's systems shall employ a method for modification of data that allows historical versions to be maintained and accessed. The Contractor shall support a “never delete a record” approach.

32.10.2. Requirement Stage: All Contract Stages

32.11. Reference #2232: When converting claim history from incumbent contractor, provide a solution that ensures all existing Transaction Control Numbers (TCNs) are maintained on the original claim.

32.11.1. Contractor Approach: The Contractor shall develop, maintain and execute a Data Conversion plan which describes planning, development, testing, coordination, and processes required to seamlessly migrate claims data from the current vendor and its vendor systems to the pharmacy system. The Contractor shall work with each data source and target system including the Department system(s), data warehouse, decision support, business intelligence, and other identified vendors to ensure all existing TCNs are maintained on the original claim.

32.11.2. Requirement Stage: PBMS Implementation Contract Stage

33. TECHNICAL REQUIREMENTS

33.1. Reference #2233: Provide scalable IT infrastructure with role based capability to establish user credentials and permissions.

33.1.1. Contractor Approach: The Contractor shall deploy a secure scalable IT infrastructure with role based capability to establish user credentials and permissions. Any user requesting access to any environment for any purpose shall receive at least two levels of approval, based on their position and role. The Contractor shall ensure that all permissions are processed appropriately, using approved protocols. The Contractor’s security procedures shall ensure unique user identifications (UUI), enforce password guidelines, and ensure role-based access, including the performance of authentication against active directory services for all applications assessed via the web (intranet or internet).

33.1.2. Requirement Stage: All Contract Stages

33.2. Reference #2234: Procure and maintain infrastructure hardware and software including upgrades and technology refreshes to maintain functionality of all interfaces.

33.2.1. Contractor Approach: The Contractor shall be responsible for procuring the hardware and software needed for a successful operations and maintenance throughout the term of the Contract. The Contractor shall be responsible for reviewing and maintaining current technology for supported interfaces including upgrades. The Contractor shall manage the associated, maintenance and licensing agreements for the purchases made. The licensing procurements shall accurately reflect the design and usage requirements of the software purchase. The Contractor shall properly install all service packs, revisions and patches are and for ensuring that proper installation instructions are followed and coordinated with the Department.

33.2.2. Requirement Stage: All Contract Stages

33.3. Reference # 2235: Provide the ability for an authorized System user to have Single Sign-On access, interface, and/ or linkage to various resources and other sites/ portals as requested by the Department.

33.3.1. Contractor Approach: The Contractor shall provide the ability for an authorized System user to have SSO access, interface, and/ or linkage to various resources and other sites/ portals as requested by the Department. The Contractor shall collaborate with the Department to identify roles specific to Department data and application access needs. The Contractor shall maintain under its system access security an SSO solution. The SSO solution shall authenticate and authorized users against Active Directory/LDAP using central authentication services or participate as a service provider in a trusted network with the Department. The Contractor shall provide an appropriate Secure Web Portal for Department users to access PBMS applications and other Web content using SSO.

33.3.2. Requirement Stage: All Contract Stages

33.4. Reference # 2236: Provide an online, viewable, indexed, and content-searchable archive with version control for all PBMS forms, documents, data files, data, and manuals to identify archived information to expedite the retrieval of archived information.

33.4.1. Using the developed index, Contractor shall be able to retrieve 95% of the information within seven (7) Business Days when requested by the authorized PBMS user.

33.4.2. Contractor Approach: The Contractor shall use document management systems, which provide a unified general content management solution that supports versioning capabilities and appropriate change control.

33.4.3. The Contractor's electronic data repository shall provide an on-line fully viewable, indexed and searchable repository for project artifacts, and put processes in place to move all documentation used to manage, deliver and operate the system into this repository.

33.4.4. Requirement Stage: All Contract Stages

33.5. Reference # 2237: Provide the ability to support different/ multiple aspect ratios and screen resolutions for PBMS displayed data, with the ability to maximize, minimize, and show multiple screen displays.

33.5.1. Contractor Approach: The PBMS shall be all Microsoft Windows and/or web based applications. As such, they shall natively support multiple screen sizes and resolutions through the operating system or the browser. In addition, both platforms shall offer the capability of running in multiple windows (or browser tabs) and to display multiple screens concurrently.

33.5.2. Requirement Stage: All Contract Stages

33.6. Reference # 2238: Provide takeover information archives in a manner that facilitates fast and accurate information retrieval including a viewable, indexed, and content-searchable format.

33.6.1. Contractor Approach: The Contractor shall store all artifacts in a document management system. The document management system shall allow the Contractor to export the content stored within it to be viewable, indexed, and searchable format.

33.6.2. Requirement Stage: All Contract Stages

33.7. Reference # 2239: Provide the ability to automate the meta-tagging of documents based upon their contents, and to allow user defined meta-tags.

33.7.1. Contractor Approach: The Contractor shall utilize a document management system that supports the automatic meta-tagging of documents based on their content types. The Contractor shall configure the document management system to automatically add metadata to documents when they are uploaded to the document management system based on the workflow from which the document came or some other context. The Contractor shall also allow user defined metadata to be added to document in the document management system.

33.7.2. Requirement Stage: All Contract Stages

33.8. Reference # 2240: Provide the ability to create and maintain multiple group-based Customized display environments of System information so that a group sees only the information the group wants or is allowed to see, in the order that the group desires to see it.

33.8.1. Groups may be business units, or may be defined by job category, employee status (e.g., permanent, temporary, new hire pre-HIPAA training), or other Department defined criteria.

33.8.2. Contractor Approach: The PBMS shall support role/group based security and allows a system administrator to configure the contents of each screen based on security groups. The Contractor shall configure the PBMS so that roles/groups are only able to see information that the Contractor, in collaboration with the Department, determines are appropriate for that group to view.

33.8.3. Requirement Stage: All Contract Stages

33.9. Reference # 2241: Provide the ability to generate and track internal messaging notes between System administrators regarding an authorized System user’s profile. Include maintenance features for each message, such as update and delete, as well as a date/ time stamp and the authorizing user name for each message.

33.9.1. Contractor Approach: The Contractor shall provide a process by which a user's request for a modification to their profile triggers a security workflow. This workflow shall include sign-off from the Contractor's supervisory staff appropriate to the particular user and/or to the type of data to which the user has requested access. While the process is taking place, the Contractor's system administrators shall be able to make notes and exchange messages amongst themselves. In addition Contractor's system administrators shall utilize the Contractor’s secure email system to communicate with other participants in the workflow who do not have access to the help desk system. In either case, the Contractor's communication shall include a date/time stamp and the user who originated the message.

33.9.2. Requirement Stage: All Contract Stages

33.10. Reference # 2242: Provide the ability to troubleshoot and debug data processing errors (e.g., if a user-input change was not accepted by the PBMS, or if a value was changed within the PBMS without authorization).

33.10.1. Contractor Approach: The Contractor shall provide two places where corrections can be done for the troubleshooting and debugging of errors: in the plan administration GUIs, and also to the actual feeds. The Contractor will receive clear and explicit authorizations with detailed corrective steps from state/MMIS in the event manual corrections to data received externally are required.

33.10.2. Requirement Stage: All Contract Stage

33.11. Reference # 2243: Support the functionality to trigger electronic correspondence to client, provider, submitter, and Contractor by email distribution, fax, posting, automated letter generation (using standard letters or forms, letter templates, and free-form letters), as well as interface with automated correspondence generation functionality.

33.11.1. The Contractor shall not inappropriately distribute PHI or PII.

33.11.2. Contractor Approach: The Contractor shall utilize its enterprise correspondence generation system along with the Contractor's corporate print shop facilities. The correspondence generation system shall support the creation of electronic documents which can then be printed, faxed or otherwise distributed to the recipient.

33.11.3. Requirement Stage: All Contract Stages

34. SYSTEM INTERFACES

34.1. Reference # 2244: Provide the ability to electronically scan all paper claims/ encounter claims data and interface with the MMIS Electronic Data Management System (EDMS) process.

34.1.1. Contractor Approach: The Contractor shall scan all paper claims/encounters when they are received then subsequently process them in the PBMS. The Contractor shall provide an interface by which the claims data is transmitted to the MMIS.

34.1.2. Requirement Stage: All Contract Stages

34.2. Reference # 2245: Support the exchange of data between the System and the systems it interfaces with to facilitate business functions that meet the requirements of Department policy, and federal and State rules and regulations.

34.2.1. Contractor Approach: The Contractor shall work with trading partners such as external data and solution providers, including those that provide drug pricing, third party liability solutions, program integrity offerings and Drug Utilization Review services.

34.2.2. The Contractor shall support the exchange of either industry standard files, or agreed upon custom interfaces, routinely transmitted via FTP, using proper encryption and security protocols to protect data according to regulatory guidelines, enable each solution provider to examine, scrub, transform and load data into destination systems and databases in order to support the various processes upon which that data is dependent.

34.2.3. The Contractor shall support the exchange of either industry standard files, or agreed upon custom interfaces, routinely transmitted via FTP, using proper encryption and security protocols to protect data according to regulatory guidelines, enable each solution provider to examine, scrub, transform and load data into destination systems and databases in order to support the various processes upon which that data is dependent. The Department will enter into a license agreement with FDB providing for sufficient license use cases so that the MMIS vendor and BIDM and the Contractor may exchange data necessary to perform services. A copy of the FDB license agreement between the Department and FDB will be provided to the Contractor to demonstrate that the Contractor is permitted to exchange FDB files with the MMIS and BIDM vendors. The Contractor also shall have the ability to identify the technical operational and performance risks and challenges when engineering to interfacing with the Department's existing infrastructure and assets.

34.2.4. The Contractor also shall have the ability to identify the technical operational and performance risks and challenges when engineering to interfacing with the Department's existing infrastructure and assets.

34.2.5. The Contractor also shall have an architecture that includes the availability of an EDI gateway as well as Enterprise Service Bus capabilities that provides a means for more customizable and real or near real time exchanges at the individual record or transaction level if certain trading partners or solution integrators seek to utilize this architecture and approach rather than the more commonly leveraged Data Interface Architecture.

34.2.6. The Contractor may also leverage the Department's existing investments in information technology by integrating systems with the MMIS, as well as any third party partner systems as required. These integrations shall be accomplished through a combination of web services and batch interfaces as dictated by the details of each integration context.

34.2.7. Requirement Stage: All Contract Stages

34.3. Reference # 2246: Collaborate with the Department and other contractors to provide technical assistance to establish and support interfaces with the PBMS.

34.3.1. Contractor Approach: The Contractor shall collaborate with the Department and other contractors to provide technical assistance in establishing interfaces.

34.3.2. Requirement Stage: All Contract Stages

34.4. Reference # 2247: Provide and maintain data layout documentation, Data Dictionary, data mapping crosswalk, inbound/ outbound capability, and frequency for all interfaces. Data Dictionary shall be developed using industry best practices identified and cited by the Contractor and approved by the Department.

34.4.1. At a minimum, the Data Dictionary shall contain for each field:

34.4.1.1. Human readable/ "plain English" field name.

34.4.1.2. A field description.

34.4.1.3. Database field name.

34.4.1.4. Database table.

34.4.1.5. Field Type and length.

34.4.1.6. Codes associated with the field.

34.4.1.7. Descriptions of each code.

34.4.1.8. Original field source (e.g., CBMS, MMIS).

34.4.2. Contractor Approach: The Contractor shall provide access to an on-line view of data dictionary including data layout documentation, data mapping crosswalk and interface information in accordance with Department's specifications.

34.4.2.1. The Contractor shall have a flexible data model that allows making changes to the content of the database without changing structure. The rules-based architecture of Contractor's solution shall be sufficiently robust to handle most of the requirements of Department partners. In cases which require structural changes to the database, data dictionaries shall be provided for the modified subject areas for all systems; logical and physical model diagrams shall be provided for non-proprietary solutions developed for the Department. Data dictionaries shall be provided as an aid to report design and customer-driven ad-hoc reporting and analysis as well.

34.4.2.2. The Contractor shall place this documentation on the shared document repository where it shall be accessible to authorized Department users.

34.4.3. Requirement Stage: All Contract Stages

34.5. Reference # 2248: Provide the ability to send adjudication results for claims and encounters to the MMIS contractor.

34.5.1. At minimum the Contractor shall have the ability to send adjudication results to the MMIS contractor on a daily basis.

34.5.2. Contractor Approach: The Contactor shall exchange Claims and encounter adjudication results data with Department's MMIS partners on a daily basis so that provider payments can be processed through the next payment cycle and payment information can be updated in the PBMS system as soon as it is available.

34.5.3. Requirement Stage: All Contract Stages

34.6. Reference # 2249: Provide the ability to receive client eligibility data and managed care enrollment data from the MMIS contractor.

34.6.1. This shall occur as close to real-time as possible.

34.6.2. Contractor Approach: The Contractor shall receive client eligibility data and managed care enrollment data from the MMIS. The Contractor shall support eligibility transactions in two (2) different formats, HIPAA 834 and proprietary formats. The eligibility transactions shall be exchanged as batch transaction via secured FTP and processed as scheduled as close to real time as possible. The execution of eligibility jobs shall produce a report that can be validated.

34.6.3. Requirement Stage: All Contract Stages

34.7. Reference # 2250: Provide the ability to validate, edit and accept other eligibility files outside of CBMS/ MMIS, as identified by the Department.

34.7.1. Contractor Approach: The Contractor shall receive client eligibility files from any source in accordance with Department's requirements. The Contractor shall support eligibility transactions in both the, HIPAA 834 and proprietary formats. The eligibility transactions shall be exchanged as batch transaction via secured FTP and processed as scheduled as close to real time as possible. The execution of an eligibility job shall produce a report that can be validated.

34.7.2. Requirement Stage: All Contract Stages

34.8. Reference # 2251: For each Program Integrity (PI) and Department's contractor recovery, offset or adjustment, process adjustments for recovery in accordance with the NCPDP standards and send adjusted claims data to the MMIS

34.8.1. Contractor Approach: The Contractor shall process adjustments for recovery in accordance with the NCPDP B3 (rebill) or the B2 (reversal) and subsequent B1 (billing) transactions in the PBMS and adjust the claim to the proper paid amount. The PBMS shall assign a unique identification number for every claim that enters the system, regardless of the mode of submission.

34.8.2. The identification number shall be the master index for all claim related activity, including adjudication, reversal transaction, quantity and financial accumulations, and all claim related extracts. Reversal transactions shall contain a unique claim identification number, as well as link to the unique claim number of the original claim which was reversed. The claim identification number shall be sent in the claim file. When the claim is reversed or adjusted, that adjustment shall be sent in the claims file to the MMIS preventing an imbalance in the claims process.

34.8.3. Requirement Stage: All Contract Stages

34.9. Reference # 2252: Capture, store, and transmit to MMIS on all data elements submitted on drug related claims/ encounters from PBMS.

34.9.1. Contractor Approach: The Contractor shall capture, store and transmit all data elements submitted on drug related claims/ encounters to the MMIS on a schedule contained in the Contractor’s data interface plan, in the industry standard format. The claims extract delivery method to the MMIS shall be secured FTP.

34.9.1.1. The Contractor shall provide its data interface plan to the Department for review and approval.

34.9.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

34.10. Reference # 2253: Provide the ability to interface in real time with MMIS and/or BIDM medical health claims for determination and authorization of pharmacy claims according to medical criteria.

34.10.1. These medical criteria shall include, but are not limited to, all of the following:

34.10.1.1. HCPCS.

34.10.1.2. International Classification of Diseases Code Set 10 (ICD-10).

34.10.1.3. CPT.

34.10.1.4. Clinical guidelines.

34.10.2. Contractor Approach: The Contractor shall provide the capability of real time communication, as feasible, through secure web services with MMIS and/or BIDM, as directed by the Department, to exchange medical data during the determination process. These web services shall be exposed on an Enterprise Service Bus (ESB) which provides very granular management capabilities and monitoring tools. This real time arrangement shall allow pharmacy claims to consider medical criteria during the determination and authorization of pharmacy claims. The Contractor shall work with the Department to determine the most cost effective way to share medical data with the MMIS and/or BIDM.

34.10.3. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

34.11. Reference # 2254: Provide the ability to accept data from the BIDM and use the data to set post-processing edit(s) or flag rejected claims and indicate the reason for which the claim was rejected and pass this information on to the MMIS.

34.11.1. BIDM will provide the ability to conduct pre-payment PI reviews. The pre-payment analytics identify fraud, waste, abuse, upcoding, unnecessary services and other irregular billing or service practices. The Contractor shall receive data from the BIDM that can be used to identify claims for which payment should be suspended and the reason for the suspense.

34.11.2. Contractor Approach: The Contractor shall provide response messages to claims submitters so that they may be corrected and resubmitted for adjudication in accordance with NCPDP and industry standards. The Contractor shall work with the Department to determine edits that may be applied to deny claims and require additional review.

34.11.3. Requirement Stage: All Contract Stages

34.12. Reference # 2255: Provide the data to the BIDM to develop, produce, and maintain all reporting functions, files and data elements to meet current and future federal and State reporting requirements, rules and regulations. Modifications to federal and State reporting requirements made after PBMS implementation will be applied using the approved Change Management Process.

34.12.1. Contractor Approach: The Contractor shall deliver a complete NCPDP Post Adjudication file on a mutually agreed upon schedule, which is a standard format for the data exchange of pharmacy data. The Contractor shall work with the Department to deliver additional data so that the reporting and analytical needs of the program can be met due to modifications to federal and Department reporting requirements.

34.12.2. Requirement Stage: All Contract Stages

34.13. Reference # 2256: Capture and provide to the MMIS and/or BIDM all data that will be required to produce financial and utilization reports to facilitate cost reporting and financial monitoring of benefits and services.

34.13.1. Contractor Approach: The Contractor shall transfer any necessary financial and utilization information to the MMIS and/or BIDM, as directed by the Department, as long as doing so does not violate any licensing or confidentiality agreements Contractor has with other entities such as First DataBank.

34.13.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

34.14. Reference # 2257: Transmit all reference files to the MMIS and/or BIDM.

34.14.1. Contractor Approach: The Contractor shall transfer any necessary reference files to the MMIS and/or BIDM, as directed by the Department, as long as doing so does not violate any licensing or confidentiality agreements Contractor has with other entities such as First DataBank.

34.14.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

34.15. Reference # 2258: Provide content, including ad hoc and standardized reports, approved by the Department to the MMIS contractor for inclusion on the MMIS web portal.

34.15.1. Contractor Approach: The Contractor shall work with the Department to identify appropriate content for the Contractor to make available to the Web Portal that is provided by the MMIS Contractor. The content supplied by the Contractor shall follow a deliverable acceptance process agreed upon by both the Contractor and the Department.

34.15.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

34.16. Reference # 2259: Maintain Third Party Liability (TPL) carrier and resource files and update member and carrier information as received in the PBMS. Maintain historical TPL eligibility and coverage in the PBMS.

34.16.1. Contractor Approach: The Contractor shall ensure that TPL carrier and resource files and update member and carrier information are maintained as received. The Contractor ensures that benefits are coordinated such that the Department is always the payer of last resort. The PBMS receives TPL or other payer information from the MMIS, or other TPL eligibility services to update the client record for future cost avoidance. This shall include the TPL Carrier File with any carrier specific detail related to contacts, BIN, and other payer specific detail. TPL Carrier and resource files are used in combination to determine other health insurance for plan members. Once TPL information is loaded to the PBMS system for a member it shall be retained throughout the term of the Contract. Each record associated with member eligibility, coverage, or other health insurance (resource file data) shall be available for historical review and selection should the processed claim require the coverage associated with an earlier segment.

34.16.2. Requirement Stage: All Contract Stages

34.17. Reference #2260: Provide files to the Department's contractors for data exchanges with insurance carriers and governmental agencies for use in recoveries and utilization review.

34.17.1. Contractor Approach: The Contractor shall provide files to the Department’s contractors for data exchanges with insurance carriers and governmental agencies for use in recoveries and utilization review. The Contractor shall deliver on a mutually agreed upon schedule a claims extract in an industry standard format.

34.17.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

34.18. Reference #2261: Maintain and update Medicare participation information when received from external sources.

34.18.1. Contractor Approach: The Contractor shall integrate Medicare participation data received from external sources. The data shall be used to support processing of pharmacy claims to minimize expenditures to the Department while continuing to provide access to quality health care for its members.

34.18.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

34.19. Reference #2262: Receive a Provider Interface feed from the MMIS daily.

34.19.1. Contractor Approach: The Contractor shall setup an interface to daily receive a feed from the Department or designated third party that contains the most up-to-date information on pharmacy and prescriber providers, and the Contractor shall use that data whenever contact with the provider is required. The Contractor can support either a batch or a web service interface in order to receive the Provider feed.

34.19.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

35. RULES ENGINE

35.1. Reference #2263: Provide a Configurable rules based engine that allows for a successful PDL development process based on the Department-defined preferred products.

35.1.1. Contractor Approach: The PBMS shall be a table-driven and rules based engine supported by a relational database that results in a highly configurable benefit design.

35.1.1.1. The Contractor shall provide the configurable rules based engine PBMS to support the successful development process based on product assignment to preferred and non-preferred status in a preferred drug list (PDL), as well as Department-defined preferred products.

35.1.2. Requirement Stage: All Contract Stages

35.2. Reference #2264: Provide the ability for authorized PBMS users to identify and limit services within a Pharmacy Health Plan and by a specific client, based on utilization criteria established by the Department.

35.2.1. Contractor Approach: The Contractor shall provide a PBMS that can be easily and quickly updated by authorized PBMS users to identify and limit services within a Pharmacy Health Plan, and by a specific client, based on utilization criteria established by the Department.

35.2.2. Requirement Stage: All Contract Stages

35.3. Reference #2265: Provide the ability to reject pharmacy claims for specific services, clients, pharmacies, or prescribers (e.g., Mental health services).

35.3.1. Contractor Approach: The Contractor shall provide response messages to claims submitters so that they may be corrected and resubmitted for adjudication in accordance with NCPDP and industry standards. The Contractor shall work with the Department to determine edits that may be applied to deny claims and require additional review.

35.3.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

35.4. Reference #2266: Provide a web-based rules-based engine with the flexibility and capacity to support diverse and complex health care programs, including the ability to Configure alerts, notification triggers and pre-adjudication business rules.

35.4.1. Contractor Approach: The Contractor shall provide a fully integrated PBMS web-based rules engine to perform systematic pre-adjudication of business rules, supports customization of alerts, and notification triggers to support diverse and complex health care programs.

35.4.1.1. The PBMS shall comply with all applicable regulations, guidance, Federal and State laws-including the Enhanced Funding Requirements -Seven Conditions and Standards.

35.4.2. Requirement Stage: All Contract Stages

35.5. Reference #2267: Provide a web-based rules-based engine with the flexibility and capacity to support edits regarding high dose, standard billing units, and statistical outliers for drugs, including the ability to Configure claims/ encounter edits and pre-adjudication business rules.

35.5.1. The Contractor shall use national standards, such as the NCPDP billing unit description table, to develop this rules engine.

35.5.2. Contractor Approach: The Contractor shall provide a web-based rules-based highly configurable claims system. Contractor's system shall meet national standards including NCPDP standards and has been developed within the requirements of the MITA framework.

35.5.2.1. The PBMS shall support configuration and enforce high dose, billing units, and statistical outliers for drugs and supports claims/encounter edits and pre-adjudication business rules. the PBMS shall calculate and validate against industry standards including billing unit of measure standards including – "EA", "ML", and "GM"; rolling quantity limitations, per day quantity limits, dosage limitations, and member and plan financial obligations and maximums in the rules engine.

35.5.3. Requirement Stage: All Contract Stages

35.6. Reference #2268: Provide the ability for authorized PBMS users to create PBMS rules for business functions.

35.6.1. These functions shall include, but are not limited to:

35.6.1.1. Pharmacy Benefit Plan design, rate payments.

35.6.1.2. Exclusionary rates.

35.6.1.3. Pharmacy Benefit Plan administration.

35.6.1.4. Claims/ encounters processing.

35.6.1.5. Prior authorization.

35.6.1.6. Reference data update functions.

35.6.2. Contractor Approach: The Contractor shall provide a user-friendly system for authorized PBMS users to create PBMS rules for business functions. The PBMS shall include CMS guidelines for Service Oriented Architecture (SOA) and allow authorized PBMS users to support functions such as, but are not limited to: Pharmacy Benefit Plan design, rate payments, Exclusionary rates, Pharmacy Benefit Plan administration, claims/encounters processing; Prior Authorization; and supports Reference data update

functions. The PBMS shall apply all business logic for claims/encounter processing to meet the needs of the Department.

35.6.3. Requirement Stage: All Contract Stages

35.7. Reference #2269: Provide Department review and approval on the rules Configuration and rules engine design.

35.7.1. Contractor Approach: The Contractor shall review the rules Configuration and rules engine design with the Department and obtain approval.

35.7.1.1. All changes in rule configuration shall be managed through the Change Control process which shall include rigorous testing and requires Department approval before promoting to production

35.7.2. Requirement Stage: All Contract Stages

35.8. Reference #2270: Provide the ability to Configure rules to be date specific, including date added, date modified, start date, end date, and effective date.

35.8.1. Contractor Approach: The Contractor shall configure rules to be date specific in the PBMS. The PBMS shall be configured with the effective and termination dates associated with all records and displays via an audit trail the date added, date modified, start date, end date, and effective date.

35.8.2. Requirement Stage: All Contract Stages

35.9. Reference #2271: Produce and maintain documentation regarding all business rules, including any exception handling rules.

35.9.1. Contractor Approach: The Contractor shall produce and maintain documentation regarding all business rules including any exception handling rules. If a change requires modification to existing documentation, all documentation changes shall be made in a timely manner. Stringent document change-control methods shall ensure that all relevant information in the base documentation is retained whenever changes are incorporated into subsequent versions. When documentation changes are made, the revision number and the date the document was revised shall be updated. An internal documentation review process shall occur that validates all changes have been correctly made to the documentation in accordance with Department approved criteria and standards, as well as industry professional standards, before it is made available to the Department for review and approval. In addition, all documents shall be stored in the Contractor's shared document repository and available to authorized users from both the Contractor and the Department.

35.9.2. Requirement Stage: All Contract Stages

35.10. Reference #2272: Provide ongoing training and training documentation on any exception handling rules created or updated to satisfy the Department needs.

35.10.1. The Contractor shall provide this training at least annually

35.10.2. Contractor Approach: As exceptions rules are created to satisfy Department needs and objectives, the Contractor shall provide ongoing training and documentation to facilitate smooth transitions. The Contractor shall ensure that all Support Center

associates are made aware of plan changes and are knowledgeable of what is being implemented. The Contractor shall provide a training environment with training data for staff training purposes. This environment shall be used for all training courses and documentation needs during the Operational Readiness Phase of the project, and into operations. The lead trainer, along with technical resources as appropriate, shall ensure the training environment requirements are established and met, including ensuring the proper data is initially loaded and then refreshed on an ongoing basis. Training may be conducted on-site, via the Web, or via CBTs. The Contractor shall use Adobe Connect for web-based training and Adobe Captivate for CBTs. The Contractor shall perform periodic reviews of the plan with the Support Center associates and provide check-up training.

35.10.3. Deliverable: Annual Training and Training Documentation

35.10.4. Deliverable Stage: All Contract Stages

35.11. Reference #2273: Provide tracking and reporting of rule usage, exception usage, and when the rules fail to work as designed, and provide recommendations to resolve rule failure.

35.11.1. Contractor Approach: The Contractor shall track and report rule usage, exception usage encountered in the PBMS and when the rules fail to work, provide recommendations to resolve rule failure. The PBMS shall provide an audit trail of the rule that was used to adjudicate a claim and the result of that rule's application to the claim. During design and development, rules shall be tested in a separate development and QA environment and this audit trail shall be used to determine if the expected outcome is achieved when the claim encounters the rule. If it is determined that the rule does not perform as expected, the plan administrator shall work to debug the issue themselves, or if necessary, can escalate the issue to resolve it.

35.11.2. Requirement Stage: All Contract Stages

35.12. Reference #2274: Provide a User Interface to the Rules Engine enabling authorized PBMS users to easily connect and apply rules, as well as to view active and inactive rules.

35.12.1. The Contractor shall provide this interface for all environments.

35.12.2. Contractor Approach: The Contractor shall provide a user-friendly interface to all environments through a graphical user interface. The PBMS shall display pharmacy-related rules, including active and inactive rules, with an easily identifiable audit trail that displays the date, time, user name, and data changed, whether on-line or batch.

35.12.3. Requirement Stage: All Contract Stages

35.13. Reference #2275: Provide ability for the Department to create program specific alerts through easily defined parameters.

35.13.1. The alerts the Contractor provides the ability for the Department to make shall include, but shall not be limited to, the following:

35.13.1.1. Alerts to providers.

35.13.1.2. Alerts to clients.

35.13.1.3. Alerts to Department.

35.13.2. Contractor Approach: The Contractor shall provide a user-friendly rules based application that allows business users to control system parameters for benefit management, messaging (alerts) and those named in the industry standard that are situational or not mandated to process in a defined and control manner. This system, a table-driven and rules based engine, shall provide a user-friendly system design that provides clinically appropriate alerts and denials, along with additional detail in the supplemental message fields to facilitate the claim response. An authorized business user shall be able to customize supplemental messages for claims not meeting prior authorization requirements, preferred, non-preferred status of a product, or diagnosis requirements. Additional information conveyed through supplemental messages shall be available at the direction of the Department.

35.13.3. Requirement Stage: All Contract Stages

35.14. Reference #2276: Provide and maintain online documentation linking every business rule in the Rules Engine to the particular part of the PBMS design documents that called for the rule functionality.

35.14.1. Contractor Approach: The Contractor shall maintain online documentation for the PBMS Rules Engine linking the business rule to the rule functionality.

35.14.2. Requirement Stage: All Contract Stages

35.15. Reference #2277: Provide the ability to schedule implementation of rules into the PBMS.

35.15.1. Contractor Approach: The Contractor shall provide the ability to schedule implementation of rules into the PBMS, using effective and termination dates.

35.15.2. The Contractor shall gather functional rules into a standard template that is updated based on Department's rules. This living document shall include the schedule for implementation of rules into the PBMS.

35.15.3. Requirement Stage: All Contracts Stages

35.16. Reference #2278: Provide the ability to clone rules, modify them and then implement them as new separate rules.

35.16.1. Contractor Approach: The Contractor shall provide the ability to clone rules, modify and implement them as new separate rules in the PBMS. The flexible rules based engine shall allow expedited configuration of new rules by business users using a graphical user interface without modification of the application code.

35.16.2. Requirement Stage: All Contract Stages

35.17. Reference #2279: Provide the ability to Configure rules exception to be date specific, including date added, date modified, start date, end date, and effective date.

35.17.1. Contractor Approach: The Contractor shall configure rules exception in the PBMS. The PBMS shall configure rules exception with the effective and termination date associated with the rule. The system shall use the date to interrogate rules and all data to determine how to process the claim. Benefit configuration rule exception are stored with the date created and the date modified retaining a full audit trail.

35.17.2. Requirement Stage: All Contract Stages

35.18. Reference #2280: Provide the ability to respond to changes in the business by using business rules management, business process management, and business activity monitoring tools where practical.

35.18.1. Contractor Approach: The Contractor shall respond to changes in the business using a Change Management system. This system shall be a comprehensive tool that assists in the implementing of changes in a controlled environment and supports risk and resource assessments.

35.18.1.1. As part of Configuration management, the Contractor shall provide rules management and the Contractor shall provide business process management through reporting and analytics.

35.18.2. Requirement Stage: All Contract Stages

35.19. Reference #2281: Provide a process for a built-in multi-level rule review and approval process that will validate logic errors, conflicts, redundancy and incompleteness across business rules to identify any conflicts in business rules as they are being developed, tested, and implemented.

35.19.1. Contractor Approach: The Contractor shall perform multi-level review and approval of the PBMS to identify any conflicts in business rules as they are being developed, tested, and implemented.

35.19.1.1. The Contractor's Quality Assurance testing shall verify the proper execution of system components, including interfaces with external applications. Defects shall be documented in a structured process, and provided to the development team for correction, after which the test case is re-executed.

35.19.1.2. The PBMS shall have a regression tool that supports the creation of adjudication test cases that are group in sets to a non-production environment. At the conclusion of testing, the Department will provide approval for promotion to the production environment.

35.19.2. Requirement Stage: All Contract Stages

35.20. Reference #2282: Provide a workflow and rules approval process for the rules engine.

35.20.1. Contractor Approach: The Contractor shall provide a workflow and rules approval process for the rules engine. All changes shall be managed through the Change Management process and go through a rigorous testing process and Department approval before promoting to production.

35.20.1.1. The Contractor shall adhere to the Deliverable Submission Review and Approval Process as described and approved by the Department within the Communication Plan.

35.20.2. Deliverable: Workflow and Rules Approval Process

35.20.3. Deliverable Stage: All Contract Stages

35.21. Reference #2283: Provide the ability to set different reimbursement methodologies for pharmacies for claims/ encounters using such information as dispensing fees, provider type, and urban/ rural locations.

35.21.1. Contractor Approach: The Contractor shall provide the ability to configure different reimbursement methodologies for pharmacies for claims/encounters with dispensing fees, provider type and urban/rural locations. The PBMS shall support all state and federal pharmacy rules and regulations and deliver a configurable rules engines that support multiple configuration pricing methodologies options.

35.21.2. Requirement Stage: All Contract Stages

35.22. Reference #2284: Provide the ability to deny claims/ encounters with certain diagnoses codes.

35.22.1. Contractor Approach: The Contractor shall provide a rules engine that provides the ability to deny claims/encounters based on specific diagnoses codes and work with the Department to obtain the information from the MMIS and/or BIDM which will allow designation of a primary diagnosis. The PBMS shall use claim/encounter and patient history condition to qualify authorization and other claim/encounter determinations as designated by the Department.

35.22.2. Requirement Stage: All Contract Stages

35.23. Reference #2285: Provide the ability to have an authorized PBMS user define the encounter validation (edits) criteria for each managed care program and perform the data edits.

35.23.1. Contractor Approach: The Contractor shall allow authorized PBMS users to define edits to support encounter validation for each managed care program within the rules engine. The configuration functionality contained within the PBMS shall support encounter edits that are MCO specific by eligibility and incoming data on the claim.

35.23.2. Requirement Stage: All Contract Stages

35.24. Reference #2286: Deny claims for clients who have become ineligible for Colorado Medical Assistance program or who are not eligible for a specific services.

35.24.1. Contractor Approach: The Contractor shall utilize current and historical data provided by the Department's MMIS and stored in the member's eligibility verification and claims processing. Utilizing current and historical eligibility data stored in the database, effective and termination coverage dates shall allow the Contractor to determine if member is on file and eligible to receive pharmacy benefits provided by the Colorado Medical Assistance Program. The claim shall deny when the member fails to meet the eligibility requirements of the program or the member is ineligible to receive a specific service. When a claim is denied due to the lack of coverage or not eligible to receive the services billed, the denial response shall provide the NCPDP-compliant error code indicating ineligibility or service not covered as preventing payment. The PBMS shall maintain current and historical eligibility data for program eligibility, special program eligibility, Medicare/Buy-In coverage, and other member data required to support claims processing, eligibility verification, and reporting.

35.24.2. Requirement Stage: All Contract Stages

35.25. Reference #2287: Provide the capability to validate the client diagnosis code(s) submitted supports the service being billed.

35.25.1. Contractor Approach: The Contractor shall validate the client diagnosis code submitted supports the service being billed. The PBMS shall use diagnosis code(s) submitted on the claim, as well as data stored in the client's medical history shall be evaluated against clinical rules in the system resulting in authorization decisions within fractions of a second. The PBMS shall have the ability to incorporate data from the client's medication claims history, medical claims history, behavioral health information in conjunction with other data submitted on an incoming claim to validate the clinical appropriateness of the service being billed.

35.25.2. Requirement Stage: All Contract Stages

35.26. Reference #2288: Prior to payment, verify that the services on one or more claims do not exceed Department defined limits associated with the services or procedures established in a Pharmacy Benefit Plan.

35.26.1. Contractor Approach: The Contractor shall verify that services do not exceed Department defined limits associated with services or procedures established in the Pharmacy Benefit Plan prior to payment. Thresholds defined by the Department shall be configured in the PBMS for the Pharmacy Benefit Plan.

35.26.2. Requirement Stage: All Contract Stages

35.27. Reference #2289: Edit all benefits and services, and benefits utilization services claims/ encounters for TPL coverage prior to payment to ensure Medicaid is the payer of last resort.

35.27.1. Contractor Approach: The Contractor shall edit all benefits and services, and benefits utilization services claims/encounters for TPL coverage prior to payment to ensure Medicaid is the payer of last resort.

35.27.2. The PBMS shall edit all claims for the presence of TPL, utilizing the data on the member enrollment file, as well as editing for any voluntary information submitted that is not yet available on the member enrollment files.

35.27.3. Requirement Stage: All Contract Stages

35.28. Reference #2290: Provide the ability to edit claims/ encounters based on TPL to be treated as cost avoid or pay and chase based on the Pharmacy Benefit Plan.

35.28.1. Contractor Approach: The Contractor's system shall allow the Department the ability to customize its individual cost avoidance solution to meet the needs of the program. The system shall be able to edit claims/encounters based on TPL information on file to be treated as cost avoid or use the pay and chase based on the configuration of the Pharmacy Benefit Plan.

35.28.2. The PBMS shall receive TPL information from the MMIS or state eligibility system. Once TPL information is in the system, it shall be used to support cost avoidance processing at the point of sale and the Contractor shall assist the Department with any pay-and-chase activities. The flexibility of the PBMS shall allow the Department the ability to customize its individual cost avoidance solution to meet the needs of the program. Claims/encounters shall be able to edit based on TPL information on file to be treated as cost avoid or use the pay and chase based on the configuration of the Pharmacy Benefit Plan. This shall be done by enabling the varied cost avoidance options available in the PBMS and following a Department-approved hierarchy. The

TPL/COB functionality in the PBMS shall be highly configurable and allows the Department to eliminate unnecessary payments to submitters when other insurance has been identified, ensuring that the state is the payer of last resort. Furthermore, the PBMS shall perform COB when the provider submits TPL information, even in those cases where the Contractor does not have TPL records from the Department for that member.

35.28.3. The PBMS shall have the capability to load an unlimited number of cost avoidance records per customer. All active TPL records passed from the integrated MMIS enrollment system shall be read during claims adjudication. the PBMS shall require that each TPL record on file be cost avoided in order for the claim to yield a payable response.

35.28.4. Requirement Stage: All Contract Stages

35.29. Reference #2291: Provide the ability to perform clinical claims/ encounters edits using nationally accepted medical review criteria.

35.29.1. These medical review criteria shall include, but are not limited to, all of the following:

35.29.1.1. American Medical Association Current Procedural Terminology (CPT) guidelines (including CPT modifiers).

35.29.1.2. Health Care Common Procedure Coding System (HCPCS/ CPT) (including HCPCS/ CPT modifiers).

35.29.1.3. Diagnosis Codes - National Uniform Billing Committee (NUBC).

35.29.1.4. CMS claims/ encounters editing guidelines.

35.29.2. Contractor Approach: The Contractor shall implement the PBMS to perform clinical claims/encounters edits using nationally accepted medical review criteria. The Contractor's solution shall have a built-in clinical rules engine which applies the clinical and prior authorization decision logic performing clinical edits using nationally accepted medical review criteria. These clinical algorithms shall support multiple automated PA (AutoPA) scenarios utilizing historical data CPT procedure codes, ICD-9/10 diagnosis codes, and lab values (when available at a later date) to optimize and maximize claims/encounter editing to ensure consistent PA determinations.

35.29.3. Requirement Stage: All Contract Stages

35.30. Reference #2292: Provide the ability for authorized System users to define the services, limitations, and other aspects of a Pharmacy Benefit Plan.

35.30.1. Contractor Approach: The PBMS shall provide the ability for authorized PBMS users to define the services and create PBMS rules for business functions, including but not limited to: Pharmacy Benefit Plan design, rate payments, exclusionary rates, pharmacy benefit plan administration, claims/ encounters processing, prior authorization, and reference data update functions.

35.30.2. Requirement Stage: All Contract Stages

35.31. Reference #2293: Provide the ability to price or set reimbursement rates by provider type or other provider characteristic.

35.31.1. Contractor Approach: The PBMS shall provide the ability to set pricing algorithms to be configured at the plan, provider group, member type and/or drug level. The PBMS shall have the ability to support different payment methodologies based on characteristics of the provider and/or member type such as benefit package, and client age.

35.31.2. Requirement Stage: All Contract Stages

35.32. Reference #2294: Provide the ability to establish multiple rates and types of payment for managed care entities and maintain a history of multiple rates for multiple Pharmacy Benefits Plans associated with one Managed Care Organization.

35.32.1. Contractor Approach: The Contractor shall provide the ability to establish multiple rates and types of payment. PBMS shall support configuration of differential payment algorithms based on rates and types of payment for managed care entities and maintain a history of multiple rates for multiple PBMs associated with one MCO.

35.32.2. Requirement Stage: All Contract Stages

35.33. Reference #2295: Provide systematic ability to perform mass updates to reference files as defined by the Department, for such periodic updates.

35.33.1. Contractor Approach: The Contractor shall provide systematic ability to perform mass updates to reference files as defined by the Department.

35.33.2. Requirement Stage: All Contract Stages

35.34. Reference #2296: Provide ability for authorized PBMS users to manually update reference files as defined by the Department.

35.34.1. Contractor Approach: The PBMS shall provide the ability for authorized PBMS users to manually update reference files as defined by the Department.

35.34.2. Requirement Stage: All Contract Stages

35.35. Reference #2297: Within a Pharmacy Benefit Plan, provide the ability to group individual, ranges of codes, and combinations of code sets to define Episodes of Care or service combinations.

35.35.1. These codes sets shall include, but are not limited to, the following types of codes:

35.35.1.1. NDC.

35.35.1.2. Therapeutic Class.

35.35.1.3. Other groupings, such as GCN/GSN

35.35.2. Contractor Approach: Contractor’s system shall support more than 4,500 elements of pharmacy program management logic embedded in a configurable system architecture that enables business staff to vary them in sequence and hierarchy to define any processing rule; the system shall be capable of an unlimited number of edits. The Contractor shall provide claim aggregation or grouping at multiple hierarchy levels including those listed.

35.35.3. Requirement Stage: All Contract Stages

35.36. Reference #2298: Provide the ability for authorized System users to add, update, or delete Pharmacy Benefit Plan elements.

35.36.1. These elements shall include, but are not limited to, all of the following:

35.36.1.1. TPL information.

35.36.1.2. Pricing.

35.36.1.3. Prior Authorizations (PAs).

35.36.2. Contractor Approach: Contractor shall grant authorized system users permission to add, update and delete Pharmacy Benefit Plan elements in the PBMS through user provisioned access capabilities within the PBMS.

35.36.3. Requirement Stage: All Contract Stages

35.37. Reference #2299: Provide the ability to define claims/ encounters pricing methodology according to Department policy, CMS, national coding standards, and HIPAA/NCPDP standards.

35.37.1. Contractor Approach: Contractor shall define claims/encounters pricing according to Department policy, CMS, national coding standards, and HIPAA/NCPDP standards. The PBMS shall be a highly configurable claims adjudication engine that can fully support the Department's pricing methodology in full compliance with all standards and guidelines.

35.37.2. Requirement Stage: All Contract Stages

35.38. Reference #2300: Provide the ability for authorized PBMS users to set and override Pharmacy Benefit Limits.

35.38.1. The limits that the authorized PBMS users may override shall include, but shall not be limited to, all of the following:

35.38.1.1. Over-the-counter (OTC) limits.

35.38.1.2. Quantity limits.

35.38.2. Contractor Approach: The Contractor shall provide authorized PBMS users the ability to set and override Pharmacy Benefit Limits. The PBMS shall provide a user-friendly interface to access and retrieve data, set limits, and perform overrides for edits including but not limited to over-the-counter (OTC) and quantity limits.

35.38.3. Requirement Stage: All Contract Stages

36. WORKFLOW MANAGEMENT

36.1. Reference #2301: Provide a workflow engine that supports workflow access, assignments, and execution for all essential components of the business processes.

36.1.1. Contractor Approach: The PBMS shall allow access to a workflow engine for the execution for all essential components of the business processes that include contact management, prior authorizations, rebate administration, change management and claims processing. Each component of the PBMS shall have its workflow built into that component.

36.1.2. Requirement Stage: All Contract Stages

36.2. Reference #2302: Provide Department access to workflow monitoring that includes indicators and statistics by sub process, organization, or individual staff.

36.2.1. Contractor Approach: The workflows in the PBMS shall be segregated by job junction and users in the management role are given access to monitor all of the items in each workflow including information about each specific user who may have interacted with the item. The Contractor shall make this monitoring functionality available to designated Department staff. Specific monitoring functionality shall include:

36.2.1.1. Contact Management – Monitor Work Queues

36.2.1.2. Prior Authorization – Monitor Work Queues

36.2.1.3. Rebate Administration – Dashboard

36.2.1.4. Change Management – Ticket Queue

36.2.1.5. Claims Processing – View Audit Logs

36.2.2. Requirement Stage: All Contract Stages

36.3. Reference #2303: Support workflow management for multiple simultaneous processes.

36.3.1. Contractor Approach: The PBMS shall support workflow management for multiple simultaneous processes.

36.3.2. Requirement Stage: All Contract Stages

36.4. Reference #2304: Provide the ability to create workflows that route and assign cases to the appropriate staff.

36.4.1. Contractor Approach: All workflows within the PBMS that require assignment shall be assigned to appropriate staff.

36.4.2. Requirement Stage: All Contract Stages

36.5. Reference #2305: Support supervisory functions for workflow management such as, prioritization, delegation and re-routing.

36.5.1. Contractor Approach: The PBMS shall support supervisory functions for workflow management such as prioritization, delegation and re-routing.

36.5.2. Requirement Stage: All Contract Stages

36.6. Reference #2306: Provide the ability to assign caseload “weights” to cases, PI requests, or PAR requests based upon difficulty or other criteria such as complexity and priority.

36.6.1. Contractor Approach: Contractor's shall provide PBMS users in the management role the ability to route cases to specific specialists based on criteria such as expertise or availability. Such ‘weighting’ of cases, program integrity or PAR requests shall allow for the prompt processing and resolution when special consideration is required. Also, weights shall be typically related to the prioritization of individual cases so that they rise to the top of a backlog and are resolved promptly. The Contractor’s process design and Contractor's staff shall be defined to the purpose of limiting or in many cases, eliminating backlog.

36.6.2. Requirement Stage: All Contract Stages

36.7. Reference #2307: Provide the ability to assign authorized PBMS users and manage capacity levels to personnel at the agency or program level, PAR reviewers or PI reviewers.

36.7.1. Contractor Approach: Contractor's Support Center management staff shall closely monitor the queues and shall manage priorities. The support center shall manage a queue specific to the job function of Program Integrity (PI). In case the prioritization of an issue is required the case shall be able to be routed to the appropriate queue, such as PI or PAR, so that it will get the proper attention. The Contractor shall offer PBMS users in the management role the ability to route Prior Authorization and PI cases to specific specialists based on criteria such as expertise or availability.

36.7.2. Requirement Stage: All Contract Stages

36.8. Reference #2308: Provide an automatic real time update process as tasks are completed.

36.8.1. Contractor Approach: The Contractor's PBMS shall provide automatic real time updates for select tasks as they are completed. Within the PBMS select tasks will also automatically move from completed (resolved) status to closed status based on defined parameters indicating a final and unchangeable status for the selected task.

36.8.2. Requirement Stage: All Contract Stages

36.9. Reference #2309: Create work items in workflow as a result of automated alerts when defined changes occur.

36.9.1. Contractor Approach: The Contractor shall provide a PBMS that maximizes the automated collection of information then executes a workflow to control the activities necessitated by the defined changes that occur.

36.9.2. Requirement Stage: All Contract Stages

36.10. Reference #2310: Establish Training Workflow for authorized PBMS users.

36.10.1. Contractor Approach: The Contractor shall create training workflows for authorized PBMS users for each system application. These workflows shall be documented in step-by-step job aids, computer- based tutorials (CBTs), and training user manuals.

36.10.2. Requirement Stage: All Contract Stages

36.11. Reference #2311: Integrate PBMS workflow management processes with Department utilized office productivity applications to support process execution. Integration with these applications shall be done by leveraging the productivity application's database, or through the use of output files generated by the productivity application.

36.11.1. Department utilized office productivity applications may include, but are not limited to, the following:

36.11.1.1. Microsoft Office products.

36.11.1.2. Computer Associates Clarity software.

36.11.1.3. Microsoft SharePoint.

36.11.2. Contractor Approach: The Contractor shall work with the Department to determine the specific workflow processes that shall be integrated with the Department's office

productivity applications. The Contractor shall integrate with the Department's office productivity applications through the use of output files generated from the Contractor's system.

36.11.3. Requirement Stage: All Contract Stages

36.12. Reference #2312: Provide authorized PBMS users the ability to monitor, intervene in and resolve rules based actions or unexpected failures.

36.12.1. These abilities shall include, but are not limited to, all of the following:

36.12.1.1. Ability for the PBMS to display and to generate "pull lists" or "to-do" lists.

36.12.1.2. Ability to transfer pull lists and to-do tasks to other authorized PBMS users.

36.12.1.3. Ability for a business user to create PBMS rules to route issues.

36.12.1.4. Ability to keep a diary or log of the investigations into the actions, and their resolutions.

36.12.1.5. Ability to track resolutions over time to identify trends and patterns.

36.12.1.6. Ability for management to monitor the workflow (duration) and caseloads (volume) of the reviewers and others in the edit workflow process.

36.12.1.7. Ability for reviewers to assign tasks and reminders to other authorized PBMS users.

36.12.1.8. Ability to report on reviewer assignments and workloads.

36.12.2. Contractor Approach: The Contractor shall provide functionality in the PBMS that will allow users to monitor, intervene in and resolve rules based actions or unexpected failures. Examples of such functionality shall include but not be limited to:

36.12.2.1. SX Monitor – On a 24x7 basis claims processing shall be monitored. If measured metrics fall below configurable criteria, automated alerts shall be sent to contractor personnel who will initiate workflows to diagnose and resolve the issue.

36.12.2.2. Rebate – Contractor's rebate system shall be based on workflow. The system shall generate work queues, logs the actions taken by users, and allows management to monitor the workflow.

36.12.2.3. Call Center - The workflows in the call center application shall be able to be displayed in queues that can be viewed and modified by authorized users so that work items can be reassigned in cases where the standard rules governing workflow must be superseded for an individual, unique case. All activities in a work item shall be saved in the Contact Record in the PBMS so there is a permanent record of all notes, activities, resolutions, and communications surrounding a work item.

36.12.2.4. Automated reporting for batch loads – The Contractor shall provide a system that monitors the process of loading batch files and reports the output to contractor personnel who will initiate workflows to diagnose and resolve the issue.

36.12.2.5. Change Management Process – Contractor shall provide a change management system that shall route requests though a workflow that provides the delivery of alerts, the ability to route requests manually, and to record approvals attributable to authorized users.

36.12.3. Requirement Stage: All Contract Stages

36.13. Reference #2313: Allow authorized PBMS users to submit requests to update PBMS profiles which initiates a workflow for the Department to approve, as necessary.

36.13.1. Contractor Approach: The Contractor shall maintain a change control process that shall govern system changes to ensure auditability, facilitate communication and to mitigate risk. An integral part of Contractor's change control process shall involve communicating with and receiving sign off from Department. Items that are covered by change control process shall include but are not limited to security requests that would modify a user's profile to gain access to Department resources, changes to benefit configuration, changes to prior authorization rules in the clinical decision module or enhancements to Contractor's software tools.

36.13.2. Requirement Stage: All Contract Stages

36.14. Reference #2314: Automatically and securely route grievances and appeal requests to the authorized PBMS users or user groups for multiple levels of review, per business rules.

36.14.1. Contractor Approach: The PBMS shall have call tracking items (CTIs) for grievances and appeals. These CTIs shall be automatically set into specific queues and then managed by appropriate personnel based on the details configured in the workflow for that CTI.

36.14.2. Requirement Stage: All Contract Stages

36.15. Reference #2315: Provide an on-line, real-time communications tracking tool with role-based access to monitor and document System updates, day-to-day business, and exchanges between Contractor(s) and the Department.

36.15.1. Contractor Approach: The PBMS shall facilitate the communication between all interested parties including Department designated users. The PBMS shall offer role based access and track correspondence between system administrators and end users in the domain of system architecture and network administration such as system updates.

36.15.2. Requirement Stage: All Contract Stages

36.16. Reference #2316: Provide the ability to collaborate on documentation (e.g., system, project, provider communication materials) via editing capabilities. Include the ability to limit editing of certain documents by type and/ or origination. Track and maintain version history of documents and related attachments that have been edited.

36.16.1. Contractor Approach: The Contractor shall use a document management system as the shared document repository and as a collaboration tool. The system shall allow the Contractor and the Department staff to share documents of various types and associated actions by user role and document type. The shared document repository shall be capable of managing and tracking version history. Documents access shall be limited by the role of the authorized user.

36.16.2. Requirement Stage: All Contract Stages

37. DATA MANAGEMENT

37.1. Reference #2317: Data management within the PBMS and the Contractor's operational policies and practices shall:

37.1.1. Meet HIPAA, HITECH, ARRA and other federal and State privacy and security requirements as they currently exist and be Configurable to assist in meeting future requirements.

37.1.2. Ensure security, accuracy, and timeliness of data interfaces.

37.1.3. Incorporate electronic and digital signatures that comply with HIPAA and State law.

37.1.4. Contractor Approach: The Contractor's core data management systems shall be fully compliant with Title II, Subtitle F, Section 261-264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, titled "Administrative Simplification" and the rules and regulations promulgated. The PBMS shall meet all federal requirements as prescribed by CMS, the requirements outlined by the National Archives and Records Administration Code of Federal Regulations (CFR) parts 42 and 45, and standards for ProDUR. The Contractor's policies and procedures shall be written to ensure the employees understand and adhere to the proper handling, use, and disclosure of protected health information (PHI) and confidential information while administering health care benefits and providing an appropriate level of customer service.

37.1.5. Data management within the PBMS and the Contractor's operational policies and practices shall:

37.1.5.1. Meet HIPAA, HITECH, ARRA and other federal and State privacy and security requirements as they currently exist and be Configurable to assist in meeting future requirements.

37.1.5.2. Ensure security, accuracy, and timeliness of data interfaces.

37.1.5.3. Incorporate electronic and digital signatures that comply with HIPAA and State law.

37.1.6. The Compliance and Regulatory programs of the Contractor shall demonstrate that employees, including any subcontractors, are aware of and adhere to, the provisions of HIPAA privacy and security policies and procedures.

37.1.7. Requirement Stage: All Contract Stages

37.2. Reference #2318: Contractor shall maintain:

37.2.1. Data Confidentiality – Prevent disclosure to unauthorized persons or systems.

37.2.2. Data Integrity – data cannot be modified undetectably.

37.2.3. Data Availability – access is not inappropriately blocked or denied.

37.2.4. Data Authenticity – validation of transactions.

37.2.5. Data Security – encryption and Department approved security protocols and processes.

37.2.6. Non-repudiation of Data – parties to a transaction cannot deny their participation in the transaction.

37.2.7. Contractor Approach: The Contractor shall implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the electronic PHI generated, received, maintained, or transmitted on behalf of the Department. These measures shall be included in the Privacy and Security Compliance Program, as well as security and HIPAA privacy policies and procedures with which all Contractors and subcontractors shall comply:

37.2.7.1. Data Confidentiality – The Contractor shall maintain documented policies and procedures to ensure the proper handling, use, and disclosure of protected health information (PHI) and confidential information while administering health care benefits and providing an appropriate level of customer service. The Contractor shall limit access to systems and applications to authorized users only. The Contractor shall engage a Compliance Director to be responsible for oversight of Compliance and Regulatory programs and for ensuring that employees, including any subcontractors, are aware of and adhere to, the provisions of HIPAA privacy and security policies and procedures.

37.2.7.2. Data Integrity – The Contractor shall maintain strict control over approving users that will have access to add or alter data. Security configurations shall allow only permitted users (Department-designated or from the Contractor) to create or modify data within the PBMS. The Contractor shall maintain an audit log of all actions performed on PHI. The Contractor shall ensure all critical audit information is captured when the actions occur.

37.2.7.3. Data Availability – The PBMS system shall be available to authorized users 24 hours a day, 7 days a week throughout the year, except for approved, periodic, regularly scheduled downtime for maintenance. The Contractor shall provide the Department users access to the Contractor's 24 hour IT helpdesk to provide assistance to password resets or other Contractor network access problems.

37.2.7.4. Data Authenticity – The Contractor shall employ processes to produce load/error reports that identify number of records read and written to the database, including such items as total records received, total records processed, and details of rejected records. The Contractor shall maintain the metrics for analysis as a second level of protection against data being either manipulated or damaged in transit.

37.2.7.5. Data Security – The Contractor shall employ encryption technologies to secure data exchanges, including secure file transfer protocol (SFTP), file transfer protocol secure (FTPS), file transfer protocol (FTP) with PGP encryption, business-to-business VPN, EDI, real-time SOAP/XML exchanges, data-at-rest encryption. All encryption technologies shall at minimum use Advanced Encryption Standards (AES) minimum 128-Bit keys and be validated for Federal Information Processing Standards (FIPS) 140-2 Level 1.

37.2.7.6. Non-repudiation of Data – The Contractor shall, in partnership with the IdP, provide an Enterprise User Provisioning System that facilitates provisioning for users who work on behalf of providers, State offices, and other stakeholders. Each user shall be provided a unique ID/password when accessing applications to support non-repudiation and role-based access.

37.2.8. Requirement Stage: All Contract Stages

37.3. Reference #2319: Ensure secure and reliable data exchange across the Department's Medicaid Enterprise and with external systems to maximize data integrity.

37.3.1. This includes, but is not limited to:

37.3.1.1. A unified data exchange solution to ensure successful data exchange.

37.3.1.2. Monitors and alerts appropriate parties of potential issues.

37.3.1.3. A data model that is consistent with the Department's business processes and the Medicaid Information Technology Architecture (MITA) business processes.

37.3.2. Contractor Approach: The Contractor shall utilize a commercial level file transfer system to manage the reliable data exchange across the Department's Medicaid enterprise and with external systems to maximize data integrity.

37.3.3. Secure file transfer between parties. The file transfer systems shall have the ability to connect to diverse systems, easily transform the data to incorporate business rules and provides configurable notifications. The PBMS shall support a variety of secure data exchanges, including secure file transfer protocol (SFTP), file transfer protocol secure (FTPS), file transfer protocol (FTP) with PGP encryption, business-to-business VPN, EDI, real-time SOAP/XML exchanges, and many other forms of media. The Contractor shall support a unified data exchange solution to ensure successful data exchange by using industry standards, such as XML, NCPDP, HIPAA, and HL7 for interoperability and data integration needs. Industry standard data exchange using industry-leading tools, including Oracle Fusion, EDIFECS, and Informatica shall be implemented to manage the exchanges and reduce incompatibilities. Job monitoring and system level checks shall be instituted on all interfaces data exchanges and configured to automatically to alert appropriate parties of potential issues. The interface exchange data model shall be consistent with the Department's business processes and MITA business processes. The Contractor's supporting data base systems should be continuously reviewed and refined to best serve the PBMS business architecture a unified data exchange solution to ensure successful data exchange.

37.3.4. Requirement Stage: All Contract Stages

37.4. Reference #2320: Provide ability to accommodate data changes and/ or additions for State, federal, and administrative and clinical data structures/ elements.

37.4.1. Contractor Approach: The Contractor's systems shall be built upon a robust and mature data model that supports interfaces based on nationally recognized standards. In the event that changes become necessary, the Contractor shall support the change in the most efficient method available to the Contractor. For example, if the change results in a modification to the layout of an interface coming from the Department, the Contractor may first try to accommodate the change through an ETL process before resorting to a change to the Contractor's data model.

37.4.2. Requirement Stage: All Contract Stages

37.5. Reference #2321: Maintain the integrity of the provider data that is received from the MMIS and/or BIDM, as directed by the Department. Store the data in a way that separates

the first and last name for practitioners and provides authorized users with the ability to search by either value along with other criteria including but not limited to: Practitioner Type, Specialty, ID Type, ID, State, and ZIP Code.

37.5.1. Contractor Approach: The PBMS shall store the first and last name separately for practitioners and provide authorized users with the ability to search by either value along with other criteria including but not limited to: Practitioner Type, Specialty, ID Type, ID, State, and ZIP Code. To the extent that information comes from a system of record, the Contractor shall maintain the integrity of the data. The Contractor shall also provide flexible searches, such as allowing the use of wildcards, in key fields in the search criteria.

37.5.2. Requirement Stage: All Contract Stages

37.6. Reference #2322: Provide the ability to identify the source of data and the date added to the PBMS.

37.6.1. Contractor Approach: The Contractor shall provide the capability for users and the Department to identify whether any given change was the result of data exchange (e.g., eligibility file updates from the MMIS) or by an authorized user (e.g., adding a lock-in restriction), and the date on which the data was added or modified.

37.6.2. Requirement Stage: All Contract Stages

37.7. Reference #2323: Provide access to the PBMS for all authorized PBMS users and business partners.

37.7.1. Contractor Approach: Access to the PBMS shall be granted to authorized PBMS users and Department business partners designated and approved by the Department. The Contractor shall maintain strict control over approving users that will have access to add or alter data. Security configurations shall allow only permitted users (Department-designated or from the Contractor) to create or modify data within the PBMS.

37.7.2. Requirement Stage: All Contract Stages

37.8. Reference #2324: Provide the ability to view online the Data Dictionary information for any given System field while viewing the actual data in the System.

37.8.1. Contractor Approach: The Contractor shall make all data dictionaries available on the Contractor’s shared documentation portal so they are accessible by all authorized users. This shall enable the user’s ability to have one of the Contractor's applications open while simultaneously viewing the data dictionary opened from the repository.

37.8.2. Requirement Stage: All Contract Stages

37.9. Reference #2325: Convert all applicable data from the Department’s Legacy System and produce comparative reports for previous periods of operation of at least 3 years.

37.9.1. Contractor Approach: The Contractor shall deliver, maintain, and execute a Data Conversion Plan that describes the planning, development, testing, coordination, and processes required to seamlessly migrate data from the Department and its vendor systems to the PBMS. The Data Conversion Plan shall document the current understanding of the business processes involved in the interrelated systems as described during requirements sessions and subsequent end user clarification meetings

conducted during the requirements validation phase. The Contractor shall provide data conversion results in the agreed upon format to the Department for review

37.9.2. Requirement Stage: All Contract Stages

37.10. Reference #2326: Provide the ability to view raw interface files for up to sixty (60) calendar days.

37.10.1. Contractor Approach: The Contractor shall provide the ability to view raw interface files for up to sixty (60) calendar days. After sixty (60) calendar days interface files shall be archived for a minimum of six (6) months and the Contractor shall, upon request, make them available to the Department to review.

37.10.2. Requirement Stage: All Contract Stages

37.11. Reference #2327: THIS REQUIREMENT INTENTIONALLY DELETED

37.12. Reference #2328: Without the need for Customization, allow authorized PBMS users to add/ update valid values.

37.12.1. Contractor Approach: The Contractor shall provide the ability for an authorized user to, through configuration only, add/update valid values.

37.12.2. Requirement Stage: All Contract Stages

37.13. Reference #2329: Maintain a snapshot of client eligibility and plan enrollment information that existed at the time of claims/ encounters payment and link to the specific claim/ encounter.

37.13.1. Contractor Approach: Client eligibility spans used at the time of adjudication shall be maintained in the PBMS, linked to the claim and sent on the claims extract.

37.13.2. Requirement Stage: All Contract Stages

37.14. Reference #2330: Provide and maintain documentation for all structured data such as file layouts for pricing tables, Provider tables and Client data tables.

37.14.1. Contractor Approach: The Contractor shall make available in the shared document repository all file layouts for structured data. This documentation shall enable authorized users to review the details of exactly what is stored in the Contractor's data models and the data structures in which it is stored.

37.14.2. Requirement Stage: all Contract Stages

37.15. Reference #2331: Build and maintain a directory of all contact information of clients, providers, vendors, Department employees, and Contractor employees to support local user letter creation through data-merge in standard PC desktop applications, but still maintain Address Confidentiality PI and allow for opt-out.

37.15.1. Contractor Approach: The Contractor shall build and maintain a directory of all contact information to be used by the Contractor's enterprise correspondence publication application. The contact information shall be maintained in the Contractor's Oracle database and accessed through the Contractor's call center application which is integrated with the correspondence publication application. Correspondence shall be produced when triggered by a configured event or as part of a workflow configured in the PBMS. Opt-Out information, if available, shall be sent to the Contractor on the feed

on which each type of contact information arrived. Opt-Out information shall also be collected by the Contractor in the call center and modified through the PBMS. The Contractor may provide an extract of contact information to support letter creation through data-merge in standard PC desktop applications.

37.15.2. Requirement Stage: All Contract Stages

37.16. Reference #2332: THIS REQUIREMENT INTENTIONALLY DELETED

37.17. Reference #2333: THIS REQUIREMENT INTENTIONALLY DELETED

37.18. Reference #2334: Provide the ability to create and maintain role-based authorized PBMS user profiles to allow for the direct data entry into the PBMS.

37.18.1. Contractor Approach: The Contractor shall retain the ability to create and maintain role-based authorized PBMS user profiles to allow for the direct data entry into the PBMS. The Contractor shall collaborate with the Department to identify roles specific to Department data and PBMS application access needs. Security profiles shall be role-based and users shall receive access only to the information they need to know to do their jobs. The roles shall be well-defined within the Contractor's security policies and standards.

37.18.2. Requirement Stage: All Contract Stages

38. APPLICATION ENVIRONMENTS

38.1. Reference #2335: Provide the ability to run multiple sessions, environments, applications, areas, and views simultaneously.

38.1.1. Contractor Approach: The Contractor shall provide the ability to run multiple sessions, environments, applications, areas, and views simultaneously. The environments shall be segregated at the server and database levels allowing desktop users to attach to the application or database tiers from a single workstation. The Contractor shall deploy multiple environments as defined in the Environment Architecture and Implementation plan. The plan shall provide system architecture drawings and crosswalk tables to serve as a quick reference to the specific servers, databases, and user interface pages to help testers, plan developers, and other technical staff to attach to the appropriate systems when performing tests, plan creations, or system configuration adjustments.

38.1.2. Requirement Stage: All Contract Stages

38.2. Reference #2336: Provide all various PBMS environments necessary to perform all required functions such as testing, training, production operations, modeling, and disaster recovery.

38.2.1. These environments may include, but are not limited to, all of the following:

38.2.1.1. Multiple environments.

38.2.1.2. Multiple application layers.

38.2.1.3. Hub architecture.

38.2.2. Contractor Approach: The Contractor shall work collaboratively with the Department to design a plan for establishing the necessary environments to support the diverse user communities of the PBMS whose roles and responsibilities including tasks associated

with program and benefit development, testing, training, and/or promotion of benefit changes into production. The Contractor shall maintain the multiple development, test and training environments as well a stable well-managed production environment. Each of these environments, for selected users, shall be able to be accessed simultaneously, to allow the users to compare results between production and nonproduction environments in order to complete tasks associated with quality assurance, modeling, testing, defect analysis and benefit change impacts.

38.2.3. Requirement Stage: All Contract Stages

38.3. Reference #2337: Minimize production PBMS Configuration errors by using clear, concise, and automated business rules.

38.3.1. Configurations, data alterations, and other changes shall be moved from one PBMS environment to another to minimize PBMS Configuration errors.

38.3.2. Contractor Approach: Configurations, data alterations, and other shall be moved from one environment to another by using clear, concise, and automated business rules. The Contractor shall demonstrate the ability to maintain and operate a POS system according to documented complex automated business rules. The effective PBMS rules solution shall be table-driven and rules-based that is supported by the PBMS. Changes shall be able to be implemented by knowledgeable business users without any programming effort. Benefit configuration and maintenance shall be achieved by rules configuration and by non-technical business users by employing automated business rules processing.

38.3.3. Requirement Stage: All Contract Stages

39. SYSTEM PERFORMANCE REQUIREMENTS

39.1. Reference #2338: Provide tools that deliver asynchronous communication, timely alerts and notifications to ensure broad availability of data to authorized System users in a timely manner.

39.1.1. Contractor Approach: The Contractor's data center shall be staffed 24 hours a day, 7 days a week, 365 days a year, to ensure the ongoing maintenance and support of the IT Infrastructure and to provide asynchronous communication, timely alerts and notifications to ensure broad availability of data to authorized System users in a timely manner. Department shall have 24-hour-a-day, 7-day-a-week access to the Contractors IT Service Center (ITSC) Help Desk, ensuring any data access issue that may arise shall be handled in a swift and efficient manner. The ITSC shall maintain detailed contact information to ensure issues reported to them are escalated to the appropriate support group in a timely and efficient manner. Each group within the data center (e.g., telecommunications, network support, etc.) shall maintain on-call staff who can respond to issues that may arise at any time. Automated tools shall be deployed to continuously monitor IT infrastructure, perimeter, systems, and databases and report on issues or items that are outside of thresholds set to define optimum operation and performance. These tools shall monitor the facilities and environmental conditions, the WAN, local area network, Intel server infrastructure components, midrange systems and database systems. The Contractor shall alert PBMS users of system changes through log-in alerts and email communications.

39.1.2. Requirement Stage: All Contract Stages

39.2. Reference #2339: Ensure that unscheduled PBMS downtime (anytime the user cannot access the PBMS or carry out business functions) due to any failures is limited.

39.2.1. The following are indications that the PBMS is operating outside of acceptable performance boundaries:

39.2.1.1. Delays or interruptions in the operation of PBMS and related services caused by inadequate equipment or processing capacity.

39.2.1.2. Components not available for use by authorized PBMS users as required except during periods of scheduled maintenance. Maintenance shall only occur on Sundays between 1:00 am - 3:00 am MT unless otherwise approved by the Department.

39.2.1.3. Inability to adjudicate to a paid, denied, or suspended status, all claims received by the Department within five (5) seconds of receipt.

39.2.1.4. Screen response time in excess of defined response times in this Contract.

39.2.1.5. Inability of authorized users to create, process or store reports

39.2.2. Contractor Approach: The PBMS system shall be available 24 hours a day, 7 days a week throughout the year, except for approved, periodic, regularly scheduled downtime for maintenance. Maintenance downtime shall be taken only when necessary and shall be coordinated with the Department and shall be planned to occur on Sundays between 1:00 am - 3:00 am MT to the extent possible. The Contractor shall maintain a Data Center Operations staff to monitors real-time performance of production systems 24 hours a day, 7 days a week. The Contractor shall deploy redundancy in critical system components such as networks, servers, storage to minimize downtime. The Contractor shall communicate to the Department within 30 minutes for any interruption of claims processing or if any of the PBMS is operating outside of acceptable performance boundaries such as:

39.2.2.1. Delays or interruptions in the operation of PBMS and related services caused by inadequate equipment or processing capacity.

39.2.2.2. Components not available for use by authorized PBMS users as required except during periods of scheduled maintenance.

39.2.2.3. Inability to adjudicate to a paid, denied, or suspended status, all claims received by the Department within five (5) seconds of receipt.

39.2.2.4. Screen response time in excess of defined response

39.2.2.5. Inability of authorized users to create, process, or store reports

39.2.3. Requirement Stage: All Contract Stages

40. ENTERPRISE ARCHITECTURE REQUIREMENTS

40.1. Reference #2340: Provide an approach to PBMS Configuration that can be easily updated and expanded to support changing Department needs.

40.1.1. Contractor Approach: The Contractor shall operate the POS systems, maintain benefit plans, update pricing and PA rules, and make configuration changes as needed and approved by the Department through the Change Control Process after Go-Live. A Change Control Memo (CCM) shall be initiated by the Contractor on behalf of the Department to request a change to plan configuration for items such as specific drugs, patients, providers, groups and health conditions. Following deployment to the production environment, trial claims shall be submitted to validate the edit functionality.

40.1.2. Requirement Stage: All Contract Stages

40.2. Reference #2341: Promote an enterprise view that supports enabling technologies that align with State and nationally recognized Medicaid business processes and technologies.

40.2.1. Contractor Approach: The Contractor shall make MITA maturity a priority in all business and system architecture decisions. The Contractor's priority shall be evidenced by examples including but not limited to ongoing vendor self-assessments, maintenance of a MITA roadmap and collaboration with the Department to increase the program's MITA maturity by leveraging the Contractor's capabilities.

40.2.2. Requirement Stage: All Contract Stages

40.3. Reference #2342: Provide an architecture that clearly defines service end points that add functionality without requiring pervasive or broad changes to the PBMS.

40.3.1. Contractor Approach: The Contractor shall leverage where ever possible existing functionality through currently deployed web service endpoints. The Contractor shall continue to build upon its Service Oriented Architecture (SOA) in areas that are identified as appropriate and mutually beneficial in order to avoid pervasive or broad changes to the PBMS.

40.3.2. Requirement Stage: All Contract Stages

40.4. Reference #2343: Provide a scalable and open architecture, which can interface with other systems upon implementation and in the future as required by the Department.

40.4.1. Contractor Approach: The Contractor shall provide a system that is scalable because it is deployed on an infrastructure that allows computing and storage resources to be added as necessary to support an increased need by the Department. The Contractor shall provide a system that supports nationally recognized data interface standards so that it may be interoperable with other systems which support those same standards.

40.4.2. Requirement Stage: All Contract Stages

40.5. Reference #2344: Provide a service-based architecture that makes it possible to implement common interoperability and access across the Medicaid Enterprise, including other applications, other agencies, federal and State systems, or by other new systems as needed.

40.5.1. Contractor Approach: The Contractor shall provide a system that is able to interoperate with other systems through web services. The Contractor shall utilize its Enterprise Service Bus to securely expose web services for use by other applications, other agencies, federal and State systems, or by other new systems both inside and outside of the Contractor's firewall.

40.5.2. Requirement Stage: All Contract Stages

40.6. Reference #2345: Ensure components will integrate with the overall enterprise.

40.6.1. The Contractor shall ensure these components integrate to:

40.6.1.1. Provide convenient, instant access to current and historical information without requiring a separate sign-on beyond the initial authorized PBMS user sign-on.

40.6.1.2. Employ a security approach that integrates with other PBMS components to provide role-based access with a single log-on.

40.6.1.3. Integrate with and provide support to other PBMS components as defined by the Department.

40.6.1.4. Produce status reports and processing statistics.

40.6.1.5. Ensure that all content and activity is date-stamped.

40.6.2. Contractor Approach: The Contractor shall provide a SSO experience, in partnership with the IdP, for all authorized users of the Contractor's systems through the exchange of SAML tokens. Contractor's SSO implementation shall provide role based access to all integrated systems.

40.6.2.1. The Contractor shall continually measure, monitor, and report on performance across all systems and solutions. Contractor shall instrument its important business processes so that, once live, metrics are constantly collected and evaluated to ensure that all Service Level Agreements (SLAs) and Key Performance Indicators (KPIs) are met and or exceeded. Processing statistics shall be saved in a database. The Contractor shall produce status and other reports including processing statistics.

40.6.2.2. The PBMS shall maintain a historical record and all associated changes made within the system. Each changed record shall be stamped with the user name of the person and/or load job identifier in the database making the change, along with the date and time of the change and are visible in the Graphical User Interface (GUI) for user review. Load reports shall be available for review and analysis to ensure that records have been added or updated in a timely manner. All business rules and reference file records (e.g. member eligibility record, provider record, drug records, etc.) shall include an effective and termination date in the system. Records shall never be physically deleted from the claims adjudication engine; preserving a perpetual record of all iterative changes to a record throughout the term of the Contract. Access to the audit log shall be available to users through their authorized access to the PBMS GUI.

40.6.3. Requirement Stage: All Contract Stages

40.7. Reference #2346: Provide the flexibility to create new tables and fields and to report on the data within the tables and fields as needed by transmitting all new tables and fields to the BIDM.

40.7.1. Contractor Approach: If changes are needed to support a unique Department requirement the Contractor shall use its staff of data modelers and its change management process to implement the changes and transmit the new data elements to the BIDM.

40.7.2. Requirement Stage: All Contract Stages

40.8. Reference #2347: Data from the PBMS shall be available within the System for six (6) years and archived after six (6) years, or unless otherwise directed by the Department.

40.8.1. Contractor Approach: Within the PBMS application processing data stores, the Contractor shall not purge data unless directed by the Department.

40.8.2. Requirement Stage: All Contract Stages

40.9. Reference #2348: Provide a holistic, multi-dimensional data view to the architecture requirements (i.e., a way to view simultaneously client, claim, and provider information), using the most current architecture methodology possible.

40.9.1. Contractor Approach: The Contractor's shall provide a holistic, multi-dimensional data view to the architecture requirements by ensuring its data architecture methods are based on DMBOK. The PBMS shall allow the use of a multi-dimensional data view through the use of hyperlinks and the ability to have multiple windows open simultaneously.

40.9.2. Requirement Stage: All Contract Stages

40.10. Reference #2349: THIS REQUIREMENT INTENTIONALLY DELETED

41. USER INTERFACES AND NAVIGATION

41.1. Reference #2350: Ensure compatibility with the following major web browsers: Internet Explorer, Safari, Google Chrome, and Firefox.

41.1.1. The Contractor shall support the current versions and two (2) prior versions.

41.1.2. Contractor Approach: The Contractor shall provide a system user interface that is easy to read, user-friendly, and displays all data elements necessary for a user to perform his/her job function. Careful consideration shall be given to provide the most intuitive and user-friendly design possible, while also adhering to W3C standards and 508 guidelines. The web based products shall render consistently across all current industry standard browsers and platforms including but not limited to internet Explorer, Safari, Google Chrome and Firefox, while also ensuring a pleasant interaction for the end user.

41.1.3. Requirement Stage: All Contract Stages

41.2. Reference #2351: THIS REQUIREMENT INTENTIONALLY DELETED

41.3. Reference #2352: Provide a graphical User Interface for authorized PBMS users to define plans, benefits, and pricing.

41.3.1. Contractor Approach: The Contractor shall provide a graphical user interface for Business Analysts and Plan Administrators through the PBMS. The inherent flexibility of the claims engine shall allow program edits and benefit configurations including plans, benefits, and pricing to be accomplished by working through the claim engine.

41.3.2. Requirement Stage: All Contract Stages

41.4. Reference #2353: Provide an unlimited free-form text note within the PBMS for various functions such as provider enrollment process, prior authorizations, and case management, accessible by authorized PBMS users that include:

41.4.1. The ability to display the narrative sorted by user and business unit.

41.4.2. The ability to display free form narrative in chronological or reverse chronological sequence.

41.4.3. Basic word processing functionality such as sentence case, spell check, auto text, bold, underline, italics, color font, bulleted lists, tabs, indents, wrap-text, tables, printable.

41.4.4. Contractor Approach: The Contractor shall provide word processor functionality into the notes areas of web enabled applications. This shall allow users to add multiple notes in practically unlimited free form text storage capability in the PBMS, as applicable. Once these notes are saved to the database they shall be able to be retrieved and sorted by various attributes including but not limited to user ID, business unit or entry date and in ascending or descending order.

41.4.5. As the Contractor moves ahead on MITA roadmap to web enable all applications, it shall add programming libraries that adds word processing support such as sentence case, spell check, auto text, bold, underline, italics, color font, bulleted lists, tabs, indents, wrap-text and tables to enhance its applications.

41.4.6. Requirement Stage: All Contract Stages

41.5. Reference #2354: Provide the ability for authorized users and its designees to view, search, and query by Department defined fields as well as pull reports and documentation associated with these fields.

41.5.1. Contractor Approach: The Contractor shall provide data dictionaries to the Department in the Contractor's electronic document repository. The Contractor shall also build interfaces with the MMIS and/or BIDM, as directed by the Department, so that data from the PBMS is available in the BIDM so that Department personnel may view, search, and query by Department defined fields as well as pull reports that contain pharmacy data. The Contractor shall also provide search functionality and the ability to pull reports and documentation in the PBMS.

41.5.2. Requirement Stage: All Contract Stages

41.6. Reference #2355: Provide the ability to view the results of filtered searches based on multiple or single criteria, the capability to search on multiple criteria at the same time, and the ability to perform secondary and tertiary searches within the primary search results.

41.6.1. Contractor Approach: The applications that make up the PBMS shall all contain search functionality and access shall be provided to authorized users.

41.6.1.1. Authorized users shall be able to perform searches and filter data based on one or more criteria. The search criteria shall be able to be retained to drill down the search with added criteria to accommodate search within primary search.

41.6.1.2. For use cases that are more analytical or require aggregation the Contractor shall build interfaces with the MMIS and/or BIDM, as directed by the Department, so that data from the PBMS is available in the BIDM to support analysis functionality on Pharmacy data.

41.6.2. Requirement Stage: All Contract Stages

41.7. Reference #2356: Provide the ability to view the results of wild card searches (including both single character and string wildcard search) for all searchable fields, including searches with partial ID numbers.

41.7.1. Contractor Approach: The applications that make up the PBMS shall all contain search functionality and access shall be provided to authorized users. Authorized users shall be able to perform wild card searches on searchable fields in all required screens. For use cases that are more analytical or require aggregation the Contractor shall build interfaces with the MMIS and/or BIDM, as directed by the Department, so that data from the PBMS is available in the BIDM to support analysis functionality on Pharmacy data.

41.7.2. Requirement Stage: All Contract Stages

41.8. Reference #2357: THIS REQUIREMENT INTENTIONALLY DELETED

41.9. Reference #2358: Design the User Interface to allow for the efficient keying of information into the PBMS. Efficient keying includes not requiring additional keystrokes or mouse movements, such as slashes, dashes, or double entry and context sensitive auto completion of fields.

41.9.1. Contractor Approach: To facilitate usability with the PBMS the Contractor shall work to include user interface techniques that provide the maximum efficiency for business processes. The Contractor shall web enable the PBMS, and the techniques such as the context sensitive auto completion of fields shall be introduced in selective systems as it progress on its MITA roadmap.

41.9.2. Requirement Stage: All Contract Stages

41.10. Reference #2359: Build an interface to easily allow the Department, through the PC environment such as the desktop Microsoft Word application, to data-drag provider information into merge letters.

41.10.1. The Contractor shall ensure that the interface contains:

41.10.1.1. A field for Provider names, addresses, salutations and all other information necessary to complete merge letters.

41.10.1.2. The ability to convert all uppercase information to proper format.

41.10.2. Contractor Approach: The PBMS shall provide the ability to cut-and-paste into Microsoft Office products, and through the reporting solution the PBMS shall support the mail merge and easily configurable update of letters.

41.10.3. Requirement Stage: All Contract Stages

41.11. Reference #2360: THIS REQUIREMENT INTENTIONALLY DELETED

41.12. Reference #2361: Accept digital signatures from providers on PARs.

41.12.1. Contractor Approach: The Contractor shall provide digital signature functionality to the PBMS. This shall be available prior to the PBMS Ongoing Operations and Enhancement Contract Stage.

41.12.2. The Contractor shall work with the Department to determine the exact pharmacy use cases for electronic signatures to meet those requirements.

41.12.3. Requirement Stage: All Contract Stages

41.13. Reference #2362: Support Window's based shortcuts, or similar functionality such as ctrl-c for copy and ctrl-v for paste.

41.13.1. Contractor Approach: The Contractor shall deliver systems that support Window's based shortcuts or similar functionality. To facilitate usability with application the Contractor shall include user interface techniques that provide the maximum efficiency for business processes. To that end, the team shall support Window's based shortcuts or similar functionality as a tool to increase user efficiency due to the familiarity of the shortcuts.

41.13.2. Requirement Stage: All Contract Stages

42. ONLINE HELP

42.1. Reference #2363: Propose, develop, produce, publish and deliver all applicable PBMS User Guide/ Help updates.

42.1.1. Contractor Approach: The Contractor shall provide user guides, job aids, and on-line tutorials that utilize production screenshots which display accurate representations of the application environment and are updated regularly. On-line tutorials shall allow participants hands-on training in production-style environments.

42.1.2. Contractor shall provide access to its Learning Management System (LMS) which shall house documentation for easy access to both static and dynamic information through the system's course catalog and library.

42.1.3. Requirement Stage: All Contract Stages

42.2. Reference #2364: Propose, develop, produce, and maintain frequently asked questions (FAQs) on PBMS screens and functionality.

42.2.1. Contractor Approach: The Contractor shall provide a mail box through a 'Contact Us' option on the MMIS web portal, or on the Contractor's web portal if agreed upon by the Parties, for questions and/or concerns. This mail box shall be checked on a daily basis, and response shall be supplied within 24 business hours.

42.2.2. FAQs shall be compiled into a job aid and delivered for posting to the MMIS web portal, or on the Contractor's web portal if agreed upon by the Parties, as a resource document. FAQs shall be stored in LMS Resource Library and updated on a regular basis for maximum benefit to users.

42.2.3. Requirement Stage: All Contract Stages

42.3. Reference #2365: Provide online help function to users on available shortcuts and other user-interface tips.

42.3.1. Contractor Approach: The Contractor shall employ responsive design in which pages are designed with the intelligence to configure themselves to best fit the form factor of the device. Part of this strategy shall be to employ screen elements and user interface techniques that foster usability across applications with the use of familiar elements.

42.3.2. Examples of those elements and techniques are listed below:

42.3.2.1. Online, context-sensitive help

42.3.2.1.1. Field-level tooltips, on-screen instructions, supplementary popup windows containing relevant help content, as well as a dedicated help page regarding the user experience are all provided

42.3.2.2. Hovering

42.3.2.2.1. Where appropriate, tooltips are used to provide context-sensitive feedback to the user when they hover, or mouse-over fields or interactive areas of the screen

42.3.2.3. Hypertext links

42.3.2.3.1. Hypertext links are clearly distinguished by both color and underline.

42.3.2.4. Drop down lists and menus

42.3.2.4.1. Drop down lists and menus are navigable by mouse and keyboard.

42.3.2.5. Point and click

42.3.2.5.1. Buttons, links, menus, and all other interactive areas of the screen are accessible by pointing and clicking with a mouse or other input device.

42.3.2.6. "Forward" and "Back" navigation

42.3.2.6.1. Native browser functionality for navigating forward and backward is supported.

42.3.2.7. Cut and paste

42.3.2.7.1. Cutting and pasting both from and to the application are supported.

42.3.2.8. Shortcut Keys (Ctrl+P, Ctrl+S, etc.)

42.3.2.8.1. Shortcut keys for native browser functionality are supported.

42.3.3. Requirement Stage: All Contract Stages

42.4. Reference #2366: Provide a search capability to find posts and threads by date or relevance.

42.4.1. Contractor Approach: The Contractor shall provide an on-line forum that shall enable authorized users to search among the database of forum posts to find other posts in the same thread, by date, relevance and other attributes. With role-based security, Contractor shall be able to control which users can only read the posts, which users may contribute to the forums and which users may act as moderators. If the thread is still open, users shall also be able to post questions, respond to existing questions, and create and comment on similar issues grouped together as ‘threads’.

42.4.2. Requirement Stage: All Contract Stages

42.5. Reference #2367: Provide additional functionality other than telephone, for authorized PBMS users to contact the Contractor for technical PBMS support and other questions, utilizing, for example, a “Live Chat” feature to connect the user to the Contractor's support staff via instant messaging or email.

42.5.1. Contractor Approach: The Contractor shall deploy an on-line forum as a place for authorized users to discuss program related issues. The forum shall support searching by items such as key words, date and relevance. The conversations found as a result of a search shall then be able to be continued by adding further questions or comments.

42.5.2. Contractor shall provide a Contact Us email option for questions and/or concerns. This mail box shall be checked on a daily basis, and response shall be supplied within 24 business hours.

42.5.3. Requirement Stage: All Contract Stages

42.6. Reference #2368: Provide a forum for authorized PBMS users to post inquiries, to respond to other posters and to create topical “threads” on problems.

42.6.1. The Contractor shall:

42.6.1.1. Allow Department staff and other designated users to access the forum and to participate and moderate the posts and threads, based upon user roles.

42.6.1.2. Provide a search capability to find posts and threads by date or relevance.

42.6.2. Contractor Approach: The Contractor shall provide an on-line forum that shall enable authorized users to search among the database of forum posts to find other posts in the same thread, by date, relevance and other attributes. With role based security, Contractor shall be able to control which users can only read the posts, which users may contribute to the forums and which users may act as moderators. If the thread is still open, users shall also be able to post questions, respond to existing questions, and create and comment on similar issues grouped together as ‘threads’.

42.6.3. Requirement Stage: All Contract Stages

43. ALERTS

43.1. Reference #2369: Provide messages, alerts, and a "System is down" webpage to notify users about System changes and PBMS downtimes.

43.1.1. Contractor Approach: The Contractor shall provide a notification page on the web that contains information about downtime that has been scheduled and approved. The Contractor may provide the notification page as content to the MMIS to be posted on its website at the discretion of the Department. In the unlikely event that the system experiences unscheduled downtime, the Contractor shall send an email alert to a pre-determined group of recipients notifying them that there is a problem and that the Contractor is aware of and is addressing the issue.

43.1.2. Requirement Stage: All Contract Stages

43.2. Reference #2370: Provide an exception or failure notification for batch processing and claims processing and identify a resolution process.

43.2.1. Contractor Approach: The Contractor shall produce load reports for all inbound interface executions and claims batch processing as well as automated alerts and notifications when jobs fail. All rejects shall be captured in the report. Job executions shall be monitored 24 hours a day, 7 days a week. The Contractor shall escalate failures to a published on-call number.

43.2.2. Requirement Stage: All Contract Stages

43.3. Reference #2371: Provide the ability to respond to claims with automated NCPDP edits and supplemental customized alerts to providers based on Department-defined criteria.

43.3.1. Contractor Approach: The Contractor shall configure the PBMS to respond to claims with NCPDP edits and any supplemental messages based on how its rules are configured. The Contractor shall work with the Department to develop a set of supplemental messages to be sent to providers as well as to define the conditions by which each alert will be triggered.

43.3.2. Requirement Stage: All Contract Stages

43.4. Reference #2372: Provide and maintain user-controlled and user-Configurable parameters for alerts, messages, emails, PBMS letters, and other PBMS generated notices.

43.4.1. The Contractor shall be responsible for all costs, except postage, related to PBMS letters.

43.4.2. Contractor Approach: The Contractor shall provide the capability to configure alerts and messages to the pharmacy providers through supplemental messaging. The content of the supplemental messages and the events that trigger their transmission shall be fully configurable by authorized users through the graphical user interface of the PBMS. The Contractor shall provide the capability to configure the generation of correspondence both based on workflow and based on a manual request of an authorized user.

43.4.3. Requirement Stage: All Contract Stages

43.5. Reference #2373: Alert the specified authorized PBMS user and/ or provider when a client is approaching prior authorization benefit/ service maximum.

43.5.1. Contractor Approach: The Contractor shall work with the Department to create supplemental messages to be generated when a client is approaching a prior authorization end date or a service maximum. This functionality shall be available by the Department's "go live" date. The Contractor shall provide messaging to the pharmacy provider and notification to the prescriber.

43.5.2. Requirement Stage: All Contract Stages

43.6. Reference #2374: Provide the ability for authorized PBMS users to Configure communication delivery mechanism alerts and notifications as defined by the Department, to Department staff, and Department designees.

43.6.1. The Contractor shall adhere to the Deliverable submission, review, and approval process as described and approved by the Department within the Communication Management Plan.

43.6.2. Contractor Approach: The Contractor shall provide the capability to configure alerts and messages to the pharmacy providers through supplemental messaging. The content of the supplemental messages and the events that trigger their transmission shall be fully configurable by authorized users through the graphical user interface in the PBMS. The Contractor shall provide the capability to configure the generation of correspondence both based on workflow and based on a manual request of an authorized user.

43.6.3. Requirement Stage: All Contract Stages

43.7. Reference #2375: Allow users to subscribe to, and unsubscribe from, publications and content, such as threads and hot topics, and to receive notification by email when additions or changes are made to subscribed content.

43.7.1. Contractor Approach: The Contractor shall provide an on-line discussion forum that shall enable authorized users to subscribe or unsubscribe from publications and content and to receive notification by email when subscribed content is updated. The Contractor shall gather specific requirements from the Department then configure and deploy a discussion forum and the system shall be available by the Department's "go live" date.

43.7.2. Requirement Stage: All Contract Stages

43.8. Reference #2376: Allow users to subscribe to, and unsubscribe from, publications and content such as threads or hot topics, and to receive notification by SMS, IM, or other media when additions or changes are made to subscribed content.

43.8.1. Contractor Approach: The Contractor shall provide an on-line discussion forum that shall enable authorized users to subscribe or unsubscribe from publications and content and to receive notification by SMS, IM or other media when subscribed content is updated. The Contractor shall gather specific requirements from the Department then configure and deploy a discussion forum and the system shall be available by the Department's "go live" date.

43.8.2. Requirement Stage: All Contract Stages

44. SYSTEM REPORTING

44.1. Reference #2377: Provide the ability to regularly and accurately produce operational reports using PBMS data.

44.1.1. The Contractor shall adhere to the Deliverable submission, review, and approval process as described and approved by the Department within the Communication Management Plan.

44.1.2. Contractor Approach: The Contractor shall produce operational reports and deliver them to the Department following the deliverable submission review and approval process described in the Communication Management Plan. The reports shall demonstrate adherence to Service Level Agreements as well as volumes and categories of various types of work performed.

44.1.3. Requirement Stage: All Contract Stages

44.2. Reference #2378: Ensure that the data in reports are current, accurate, and accessible and that the report is produced in a timely fashion to meet the report's delivery deadline.

44.2.1. The Contractor shall adhere to the Deliverable submission, review, and approval process as described and approved by the Department within the Communication Management Plan.

44.2.2. Contractor Approach: The Contractor shall deliver operational reports that contain current and accurate data and do so in a timely fashion according to each report's delivery deadline. The Contractor shall deliver the reports to the Department by uploading them to the shared document repository in a location accessible to the user role to whom the report is to be delivered. The shared document repository shall have

the capability for authorized users to configure alerts so that they will automatically be notified when the report is available.

44.2.3. Requirement Stage: All Contract Stages

44.3. Reference #2379: Provide complete transparency of all data fields in reports generated by the PBMS. Transparency of data fields includes, but is not limited to, providing the Department with SQL, pseudo code, narrative description, or some combination thereof to document completely the algorithms and formulas used in all reported fields and computed variables, analytic protocols and assumptions.

44.3.1. The Contractor shall maintain and provide documentation of the logic that is used to derive calculations and reports, along with descriptions of data elements used in calculations and reporting.

44.3.2. The Contractor shall have full report documentation available, human readable, and online accessible to Department.

44.3.3. Contractor Approach: The Contractor shall deliver the associated narratives and descriptors that include clearly defined metadata for all attributes of the operational reports. The documentation and artifacts assembled during the report development process shall be continuously updated with each release of the individual report or report package and provide a companion for end users to ensure full transparency and understanding of the contents of each report in the operational reporting package. During the design for each report, the Contractor shall capture the logic to be used, including, where appropriate, structured query language (SQL) or pseudo-code containing Boolean expressions, operators and operands, in the report development and design audit history. Whenever an attribute which displays on the report is a calculated attribute, the metadata for the attribute which defines the algorithms and formulas used for the attribute's calculation shall be defined and documented in order to contribute to providing complete transparency for all reports generated in support of the PBMS. Documentation for the operational reporting packages is maintained by the Contractor in an on-line, web-based document repository and is made available to end users upon request.

44.3.4. Requirement Stage: All Contract Stages

44.4. Reference #2380: Create and maintain a suite of Contractor-defined on-line reports which allow users to choose from multiple pre-built defined parameters such as: provider number, procedure code, and date of service (singly or in combination), to generate user Customized results that help users monitor the daily operations of the PBMS and PBMS Operations.

44.4.1. Contractor Approach: The PBMS shall include a web-based portal that contains both a set of pre-developed parameter driven management reports as well as a toolset enabling a subset of advanced users to define and build their own re-usable queries with the Contractor's intuitive self-service feature. Contractor shall support the BIDM in business intelligence, reporting and analytical needs through the provision of PBMS data.

44.4.2. Requirement Stage: All Contract Stages

44.5. Reference #2381: Provide the ability to generate a summary of historical file transfers.

44.5.1. Contractor Approach: The Contractor's FTP solutions shall maintain historical information for the prior 90 days of data transfers on-line and additional historical information in archived backups. In the event that a summarization of historical file transfers were necessary, Contractor shall retrieve key attributes for those historical transfers in order to support diagnosing and resolving any issues that compromise the programs interoperability objectives. At the Department's request, the Contractor shall provide data to a variety of the Department's trading partners on a routine and regular basis. As problems may arise throughout program operations, there may be occasions where troubleshooting amongst these trading partners is necessary, in order to identify whether historical data has been properly processed according to agreed-upon schedules.

44.5.2. Requirement Stage: All Contract Stages

44.6. Reference #2382: Ensure that all codes and abbreviations used in the PBMS have corresponding and easy-to-view narrative descriptions.

44.6.1. Contractor Approach: The PBMS shall leverage a robust set of data in an expansive relational database structure. Within this database, code sets and their associated narrative descriptions shall be stored so that PBMS users are able to easily view the meanings for various codes that are used to represent such things as claims status, pricing type and NCPDP error codes as well as key codes and identifiers for Members, Providers and Drugs. The Contractor shall demonstrate to the Department that all codes and abbreviations used have corresponding and easy-to-view narrative descriptions.

44.6.2. Requirement Stage: All Contract Stages

44.7. Reference #2383: Ensure that any reporting functionality supports the ability to pull and use the narrative descriptions of codes and abbreviations in addition to the codes and abbreviations themselves.

44.7.1. Contractor Approach: In order to support the BIDM reporting capabilities, Contractor shall provide a wide range of data sets that include code sets, narrative descriptions and abbreviations as necessary, in order to provide the BIDM solution provider with all pharmacy specific data necessary to support the full range of management, financial, operational and analytical reporting services. The Contractor shall also provide this functionality within the PBMS itself for reporting and search functionality.

44.7.2. Requirement Stage: All Contract Stages

45. OTHER TECHNICAL REQUIREMENTS

45.1. Reference #2384: Provide Optical Character Recognition (OCR) to convert appropriate paper documentation received through PBMS Operations into indexed, content searchable electronic format such as claims and attachments, correspondence, provider information.

45.1.1. Contractor Approach: The Contractor shall use imaging solutions, such as InfoImage, Kofax Capture, and Microsoft SQL server to enable workflow, document imaging, and management, as well as the management of e-forms.

45.1.2. The Contractor's staff shall utilize OCR capabilities to convert data contained in images into pharmacy system data. The Contractor shall use the OCR capabilities of a solution

such as Kofax Capture, which shall allow paper and fax based forms to be stored as images within the PBMS. Images shall then be associated with the claim, indexed and made searchable to PBMS systems users.

45.1.3. Requirement Stage: All Contract Stages

45.2. Reference #2385: THIS REQUIREMENT INTENTIONALLY DELETED

45.3. Reference #2386: Present authorized System users with the latest revision of a document with the option to view previous versions.

45.3.1. Contractor Approach: The Contractor shall provide a shared document repository. The shared document repository shall have the capability to maintain current and prior versions of documents. Authorized users shall be capable of viewing prior versions of each document.

45.3.2. Requirement Stage: All Contract Stages

45.4. Reference #2387: Perform batch control and reporting. The TCN assignment shall be coordinated with the Core MMIS and Supporting Services Contractor for length and non-duplication for claims/ encounters.

45.4.1. Contractor Approach: The Contractor shall have the capability to create a unique TCN and shall coordinate with the MMIS and Supporting Services Contractor to produce a unique TCN based on the Department's requirements. The Contractor shall be capable of using fields such as Julian date, media type, batch no, sequence number, and others to create TCNs. This shall include batch control and reporting.

45.4.2. Requirement Stage: All Contract Stages

45.5. Reference #2388: THIS REQUIREMENT INTENTIONALLY DELETED

45.6. Reference #2389: Allow flexibility to support Pharmacy Benefit Plan geographical service areas, by county, city, zip code, mileage, census tract, longitude and latitude, or various combinations.

45.6.1. Contractor Approach: The PBMS rules engine shall provide flexibility to support a configurable Pharmacy Benefit Plan geographical service area. The rules configuration shall cause the system to make adjudication decisions, based on county, city, zip code, mileage, census tract, longitude and latitude, or various combinations, to vary the plan based on the location of the member or of the pharmacy. The flexibility of the geographical service area rules based solution for the Department shall be modifiable to quickly to account for changes in plan rules surrounding the geographical location of members or of pharmacy providers.

45.6.2. Requirement Stage: All Contract Stages

45.7. Reference #2390: Provide the ability to track and maintain changes to postings, newsletters, and bulletins.

45.7.1. Contractor Approach: The Contractor shall use a document management system, which provides a unified general content management solution that supports versioning capabilities and appropriate change control for maintaining postings, newsletters and bulletins, and interface it with online services to publish the most updated versions.

45.7.2. Requirement Stage: All Contract Stages

45.8. Reference #2391: THIS REQUIREMENT INTENTIONALLY DELETED

45.9. Reference #2392: THIS REQUIREMENT INTENTIONALLY DELETED

45.10. Reference #2393: THIS REQUIREMENT INTENTIONALLY DELETED

45.11. Reference #2394: THIS REQUIREMENT INTENTIONALLY DELETED

45.12. Reference #2395: Update documentation based on Department requirements.

45.12.1. The Contractor shall adhere to the Deliverable submission, review and approval process as described and approved by the Department within the Communication Management Plan.

45.12.2. Contractor Approach: The Contractor shall maintain all related documentation in the electronic data repository. The Contractor shall routinely update the documents and maintain current and prior versions as determined necessary by the Department.

45.12.3. Requirement Stage: All Contract Stages

45.13. Reference #2396: Support easy-to-use data-merge functionality delivering clean contact data and Department prescribed standard texts into standard PC desktop applications.

45.13.1. The Contractor shall ensure that, at a minimum, the following functionalities are supported:

45.13.1.1. All CAPS are changed to Sentence Case.

45.13.1.2. Names, such as McNally, are properly punctuated.

45.13.1.3. Correct salutations, such as Mr. and Ms., are used.

45.13.1.4. The correct zip codes are used with addresses.

45.13.2. Contractor Approach: The Contractor shall produce correspondence using the name, Address, and demographic information in the format in which it was sent by the MMIS. The Contractor shall meet this requirement with its correspondence generation system which produces correspondence using templates created in Microsoft Word. Correspondence shall be produced when triggered by a configured event or as part of a workflow configured in the PBMS.

45.13.3. Requirement Stage: All Contract Stages

46. POINT OF SALE

46.1. Reference #2397: Provide and maintain the capability for online end-to-end processing and testing of a claim (process flow) through the PBMS and MMIS, and return processing and error messages to the submitter.

46.1.1. The Contractor shall ensure that the process flow is completed as close to real time as possible.

46.1.2. Contractor Approach: The PBMS shall provide and maintain the capability for online end-to-end claims processing and data exchange between the UAT environments of the PBMS and MMIS to allow testing of claim processing and system functionality. During claim processing and testing, claim status as well as any system generated error

messages or supplemental messaging shall be returned to the submitter for review and action.

46.1.3. Additionally, the PBMS POS claims processing component shall support the ability to perform Trial Adjudication using PBMS user submitted claims, which will processes the claim through the adjudication process in the production environment but does not save the resulting claim response. This function shall allow validation of edit functionality with no risk to the enterprise data stored in the Production environment.

46.1.4. Requirement Stage: All Contract Stages

46.2. Reference #2398: Capture, store and maintain data necessary to:

46.2.1. Correctly adjudicate pharmacy claims/encounters.

46.2.2. Perform online pharmacy claim/encounter correction.

46.2.3. Maintain and perform edits and audits.

46.2.4. Allow online pharmacy claims/encounters adjustments.

46.2.5. Allow online access to pharmacy claims/encounters history.

46.2.6. Correctly price all pharmacy claims/encounters at the detail service line and header level.

46.2.7. Allow online access to suspended pharmacy claims/encounters.

46.2.8. Provide and allow online access to pharmacy claims/encounters adjudication and status reporting.

46.2.9. Maintain pharmacy claims/encounters history.

46.2.10. Contractor Approach: The Contractor shall capture, maintain, and store pharmacy claims and encounters transactions. The Contractor shall accept electronic managed care encounter transactions for processing in the PBMS in the HIPAA named NCPDP Batch standard. The Contractor shall provide a response file to the batch submitter. The PBMS shall maintain data integrity through the strict enforcement of NCPDP field standards. Each field of incoming transaction shall be validated for data type, length, as well as submission of defined and approved values. The PBMS shall ensure that each incoming transaction is subject to syntax editing (e.g., number-only fields are numeric), and that the transaction is subject to relational editing (e.g., the submitted recipient number is on file and eligible). The system shall also ensure that the transaction data are consistent with the NCPDP field and valid code values. The PBMS shall adjudicate all claims using the same or different subset of edits/rules as defined by the Department relating to the member enrollment (Managed care versus FFS). Unless exceptions are configured, all claims (fee-for-service or encounter, MCO specific) submitted shall be subject to the same Department–specific validation and policy edits within the system and all edits shall be recorded on the claim record and made available for reporting purposes. In cases where multiple claims are sent on a single transaction, the PBMS shall be configured to ensure that only those claims that hit denial edits are returned to the provider in a non-payable state. The other claims within the transaction that do not hit any denial edits shall be processed and deemed

payable. The PBMS shall support the validation of date fields through format mask validation, but also contain edits related to date submitted versus system date.

46.2.11. Requirement Stage: All Contract Stages

46.3. Reference #2399: Provide the ability to deny claims from specific pharmacies or prescribing providers.

46.3.1. The Contractor shall ensure that requests can be prioritized into twenty-four (24) hour response or five (5) Business Day response, based on Department defined priorities.

46.3.2. Contractor Approach: The Contractor shall deny claims from specific pharmacies or prescribing providers based on Department-defined priorities. The PBMS shall be a real-time point-of-sale system, and submission of pharmacy transactions shall result in a higher first pass rate of clean claims, reducing manual intervention to re-price and track second claims to support the adjudication process. If a pharmacy claim denies upon submission and the pharmacy calls the Contractor to discuss how to resubmit the claim to get it paid the Contractor's Pharmacy Support Center staff shall assist the provider in correcting the claim so that it adjudicates appropriately. If needed or otherwise authorized, authorized business staff may make ad hoc eligibility, provider file, or pricing changes to assist in getting the claim to adjudicate appropriately per the Department's policy.

46.3.3. Requirement Stage: All Contract Stages

46.4. Reference #2400: Flag or re-price claims when requested by the Department.

46.4.1. Contractor Approach: The Contractor shall configure the PBMS per the defined requirements of the Department for flagging, re-pricing, and denying claims. If needed or otherwise authorized, authorized business staff may make ad hoc eligibility, provider file, or pricing changes to assist in getting the claim to adjudicate appropriately per the Department's policy.

46.4.2. Requirement Stage: PBMS Ongoing Operations and Enhancements Contract Stage

46.5. Reference #2401: Provide summary reports for all denied and paid and reported claims/ encounters, as requested by the Department.

46.5.1. Contractor Approach: The Contractor shall provide summary reports for all denied and paid and reported claims/encounters transactions processed in the claims adjudication system.

46.5.2. Requirement Stage: All Contract Stages

46.6. Reference #2402: Report any encounters that would have been adjudicated differently if they had been processed as fee for service claims.

46.6.1. The Contractor shall ensure that this information is delivered to the Department via a daily report.

46.6.2. Contractor Approach: The Contractor shall provide a daily report of claims/ encounters that are non-payable. The Contractor shall ensure that the report is delivered to the Department daily.

46.6.3. Requirement Stage: All Contract Stages

46.7. Reference #2403: Provide the ability to suppress claims processing based on criteria determined by the Department.

46.7.1. The Contractor's ability to suppress claims processing shall include, but not be limited to:

46.7.1.1. Suppressing all claims, certain kinds of claims, lines of service within a claim or many claims.

46.7.1.2. Suppressing claims paid on behalf of certain clients.

46.7.1.3. Suppressing payment once a ceiling amount is hit for a new provider.

46.7.2. Contractor Approach: The Contractor shall provide the PBMS to suppress claims processing based on criteria determined by the Department. The Contractor shall accomplish suppression using claim characteristics such as data fields on the claim, characteristics of the member, characteristics of the provider, and other external data sources. Contractor's system shall provide the flexibility to suppress all claims, certain kinds of claims, lines of service, as well as groups of claims.

46.7.3. The Contractor shall support the Configuration of cost ceiling edits for specific providers. The PBMS shall identify claims exceeding identified limits based on the relationship between the billed charge of the service and the new provider's price. The Contractor shall coordinate with the Department and the MMIS vendor by flagging or reporting of claims that have been approved for payment.

46.7.4. Requirement Stage: All Contract Stages

46.8. Reference #2404: Provide the ability to identify 340B claim lines, conforming to the NCPDP Standard Transactions Format, wherever possible.

46.8.1. Contractor Approach: The Contractor shall conform to the NCPDP Standard Transaction Format to process 340B claim lines. The PBMS shall accept NCPDP defined codes on submitted claims that identify 340B transactions.

46.8.2. Requirement Stage: All Contract Stages

46.9. Reference #2405: Provide selected client information back to third parties designated by the Department such as a TPL contractor or a DUR contractor.

46.9.1. Contractor Approach: The Contractor shall provide selected client data to third parties designated by the Department. Contractor shall collaborate with the Department during implementation to determine requirements.

46.9.2. Requirement Stage: All Contract Stages

46.10. Reference #2406: Provide the ability to exempt designated client from Prior Authorization requirements, when specified by the Department.

46.10.1. Contractor Approach: The Contractor shall exempt designated members from prior authorization requirements in the claims adjudication system at the direction of the Department.

46.10.2. Requirement Stage: All Contract Stages

46.11. Reference #2407: Provide the ability to post edits and deny claims/ encounters billing separately for a drug for the same client using different drug identifiers such as HCPCS or NDC numbers.

46.11.1. Contractor Approach: Contractor shall provide the ability to post edits and deny claims/ encounters from the same provider billing more than once for the same drug, member, and/ or the same claim. The Contractor shall use appropriate provider, member, and encounter and fee-for-service claims history data to ensure appropriate duplicate editing. Contractor shall provide the ability to post edits and deny claims/encounters from different providers billing separately for a drug for the same member. In the event that the Contractor receives the proper information from the MMIS, the Contractor shall deny claims in the PBMS that are duplicates of those in the MMIS at the direction of the Department.

46.11.2. Requirement Stage: All Contract Stages

46.12. Reference #2408: Provide the ability to validate the enrollment status of a prescriber or pharmacy on a claim/ encounter.

46.12.1. Contractor Approach: Contractor shall validate the enrollment status of a prescriber or pharmacy on a claim/encounter. Contractor shall load pharmacy and prescriber information, including the NPI number, into the PBMS for use in the adjudication process. As a result of loading these data to the PBMS, the Contractor's adjudication process shall have access to the most recent provider data. The PBMS shall validate pharmacy and prescribing provider information early in the adjudication process. If the submitted information does not pass the verification and validation checks, NCPDP reject messages shall be returned to the submitter with additional messaging identifying the issue to expedite a resolution.

46.12.2. Requirement Stage: All Contract Stages

46.13. Reference #2409: Provide the ability to prevent providers and prescribers from submitting claims/ encounters or verifications successfully unless the provider is actively enrolled in the PBMS. The Contractor shall make an exception to this rule with regard to report retrieval by entities that are not enrolled as billing providers.

46.13.1. Contractor Approach: Contractor shall prevent providers and prescribers from submitting claims/encounters or verification unless actively enrolled in the PBMS. Contractor shall make an exception to the rule as directed by the Department. Contractor understands there may be a need for exceptions, and shall meet with the Department during the design phase to identify system changes and business processes for exception processing.

46.13.2. Requirement Stage: All Contract Stages

46.14. Reference #2410: Provide the ability to prevent providers from submitting claims/ encounters for processing unless the provider is active and enrolled in the Core MMIS and Supporting Services.

46.14.1. Contractor Approach: Contractor shall prevent providers from submitting claims/encounters for processing unless the provider is active and enrolled in the MMIS. If the submitted information does not pass the verification and validation

checks, Contractor shall deny the transaction with NCPDP reject messages to the submitter with additional messaging identifying the issue in order to expedite a resolution.

46.14.2. Requirement Stage: All Contract Stages

46.15. Reference #2411: Enable providers to submit, inquire, and adjust claims/ encounters electronically.

46.15.1. Contractor Approach: Contractor shall enable the claim adjudication system for providers to submit, inquire and adjust claims/encounters electronically. Inquiries of claims/encounters may occur through the MMIS web portal based on information provided by the Contractor or through the NCPDP claim response and duplicate claim inquiry process.

46.15.2. Requirement Stage: All Contract Stages

46.16. Reference #2412: Maintain identifiers for designating providers who are allowed to submit paper claims or are using electronic claims/ encounters submission.

46.16.1. Contractor Approach: Contractor shall maintain identifiers for designating providers who are allowed to submit paper claims or are submitting electronic claims / encounter submissions.

46.16.2. Requirement Stage: All Contract Stages

46.17. Reference #2413: The PBMS shall maintain provider data supporting claims/ encounters processing and prior authorizations.

46.17.1. Contractor Approach: The Contractor shall maintain provider data supporting claims/encounters processing and prior authorizations.

46.17.2. Requirement Stage: All Contract Stages

46.18. Reference #2414: Provide the ability to accept National Provider Identifier (NPI) numbers from prescribers on all claims/ encounters and provide the ability to capture other ID numbers, such as DEA and NABP, where appropriate.

46.18.1. Contractor Approach: Contractor shall accept the NPI number from prescribers on all claims/ encounters and provide the ability to capture other ID numbers, such as DEA and NABP, where appropriate for processing pharmacy transactions.

46.18.2. Requirement Stage: All Contract Stages

46.19. Reference #2415: Accept and use all common, approved national standard paper claim forms.

46.19.1. Contractor Approach: The Contractor shall accept all common, approved national standard paper claim forms for pharmacy transactions.

46.19.2. Contractor shall direct data enter pharmacy submitted manual claims within 72 hours of receipt.

46.19.3. Requirement Stage: All Contract Stages

46.20. Reference #2416: Provide the ability to conduct a mass adjustment of claims.

46.20.1. Contractor Approach: Contractor shall provide functionality to conduct a mass adjustment of claims. The PBMS shall allow the user to search and select or de-select transactions prior to executing the resubmission or adjustment in production. Authorized users may submit the mass claim adjustment job as a trial job in the PBMS restore environment and review results before executing in the production environment. Claim transactions processed using this feature shall be stored in the PBMS database and shall be available for review and reporting.

46.20.2. Requirement Stage: All Contract Stages

46.21. Reference #2417: Maintain in the PBMS the unique identifier assigned by the PBMS as pharmacy claims are transmitted from the PBMS.

46.21.1. Contractor Approach: Contractor shall maintain the unique identifier assigned by the PBMS as pharmacy claims are transmitted during adjudication by the PBMS. The Contractor shall assign a unique internal identification number to each transaction.

46.21.2. The number assigned by the Contractor shall be the master index for all claim related activity, including adjudication, reversal transaction, quantity and financial accumulations, and all claim related extracts.

46.21.3. Requirement Stage: All Contract Stages

46.22. Reference #2418: Provide the ability for the PBMS to:

46.22.1. Adjust claims where payment amounts in MMIS were adjusted.

46.22.2. Perform mass adjustments on claims based on user-defined selection criteria and provide adjusted claim information to the MMIS.

46.22.3. Perform mass and individual financial adjustments based on data received from the MMIS.

46.22.3.1. The resulting claims/ encounter information will be moved into the MMIS to be stored.

46.22.4. Contractor Approach: Contractor shall perform mass and individual financial adjustments within the claims adjudication system as directed by the Department. Contractor shall support the MMIS contractor in canceling outstanding checks and/or EFT, accepting and splitting payments, and suspending and holding payments.

46.22.5. Requirement Stage: All Contract Stages

46.23. Reference #2419: Provide the ability to accept, translate and process electronic claims/ encounters transactions, and send appropriate associated responses, containing valid formats in single and batch submissions.

46.23.1. The Contractor shall ensure that it is able to do this for NCPDP Transactions.

46.23.2. Contractor Approach: Contractor shall accept, translate and process electronic claims/encounters transactions, and send appropriate NCPDP associated responses for all claims (fee-for-service or encounter, MCO specific) submitted and processes pharmacy transactions. The PBMS shall be a NCPDP – HIPAA-compliant pharmacy solution meeting all federal requirements as prescribed by CMS, as well as the requirements outlined by the National Archives and Records Administration Code of

Federal Regulations (CFR) 45 CFR Part 162 Health Insurance and supports all capturing, editing, and adjudicating processes associated with pharmacy claim and encounter processing.

46.23.3. Requirement Stage: All Contract Stages

46.24. Reference #2420: Provide a traceable and consistent unique claims/ encounter identifier. Original claims/ encounters and all subsequent adjustments shall be linked and identifiable for a consistent audit trail.

46.24.1. Contractor Approach: Contractor shall provide a traceable and consistent unique claims/encounter identifier. The PBMS shall assign all claim related activity a unique identifier, for every claim that enters the system, regardless of the mode of submission (POS, batch, paper, or interface Web). The assigned number cannot be reassigned or reused. The assigned number shall be the master index for all claim-related activity, including adjudication, reversal transaction, quantity and financial accumulations, and all claim-related extracts. Original claims shall receive one unique identifier and any subsequent adjustment to the original shall receive a separate identifier but the two claims shall be linked together. Details of all iterations of the claims transaction shall be maintained for audit purposes. Encounter claims submitted by the MCO shall also retain the MCO's unique claim identifier as well.

46.24.2. Requirement Stage: All Contract Stages

46.25. Reference #2421: Provide an audit trail that links original claim/ encounter to all adjustments.

46.25.1. Contractor Approach: Contractor shall provide an audit trail that links original claim/encounter to all adjustments.

46.25.2. Requirement Stage: All Contract Stages

46.26. Reference #2422: On all claim/ encounter records the Contractor shall retain client enrollment and eligibility information that was current for the dates of service at the time of processing the claim/ encounter.

46.26.1. Contractor Approach: Contractor shall retain enrollment and eligibility information that was current for the dates of service at the time of processing the claim /encounter. The PBMS shall maintain and display historical and current information about the member, including the cardholder ID, first name and last name, date of birth, gender, address, city, state, zip, and other member data.

46.26.2. Requirement Stage: All Contract Stages

46.27. Reference #2423: Provide a process for the storage of paper and electronic attachments associated with each claim. All information in the attachments shall be viewable and searchable.

46.27.1. Contractor Approach: Contractor shall provide a process for storing associated paper and electronic documents or attachments related to claims or prior authorization requests; all information in the attachments shall be viewable and searchable by authorized users through the PBMS. The PBMS shall link the attachment to the claim through the assignment of a transaction number.

46.27.2. Requirement Stage: All Contract Stages

46.28. Reference #2424: Provide the ability to view and search all imaged (scanned from paper) and electronic attachments associated with each claim/ encounter in the PBMS.

46.28.1. Contractor Approach: Contractor shall provide the ability to view and a process for storing associated paper and electronic claim attachments; all information in the attachments shall be viewable and searchable through the claims system. The PBMS shall link the attachment to the claim through the assignment of a transaction number.

46.28.2. Requirement Stage: All Contract Stages

46.29. Reference #2425: Provide ability for authorized PBMS users to perform claim/ encounter corrections in the PBMS. Make paid, denied, or rejected claims available for review and analysis and if deemed appropriate, allow for reversal or resubmission for the purpose of applying corrections.

46.29.1. Contractor Approach: Contractor shall provide ability for authorized PBMS users to perform claim/encounter corrections, through a resubmission of the claim/encounter, in the PBMS. The PBMS shall contain an integrated claim submission service where paid, denied, or rejected claims are available for review and analysis and if deemed appropriate, reversal or resubmission for the purpose of applying corrections.

46.29.2. Requirement Stage: All Contract Stages

46.30. Reference #2426: Support the MMIS ability for providers to generate reports that shows the full picture of their claim/ encounter activity, including their associated claims status (e.g., paid/denied) by providing claims/encounters information to the MMIS

46.30.1. Contractor Approach: Contractor shall support the ability for providers to generate reports, by providing claim and encounter pharmacy transactions with associated claims status (e.g. paid, denied) to support the MMIS's report generation.

46.30.2. Requirement Stage: All Contract Stages

46.31. Reference #2427: Provide a NCPDP/ HIPAA-compliant transmission response, such as an acceptance message or a rejection message, to the submitting provider, including managed care entities, on the success/ failure of the submission of claims/ encounters/ files.

46.31.1. The Contractor shall ensure that responses are completed as close to real time as possible.

46.31.2. Contractor Approach: Contractor shall provide real-time capture and adjudication of pharmacy claims via POS as routed via switch, direct lease line or the Internet with real time responses. Contractor anticipates virtually all encounter claims will be submitted via batch claim by the MCOs vs. real-time using the POS system. The Contractor's turnaround times shall meet or exceed the Department's requirements of adjudicating POS claims (paid or denied) within a maximum of 24 hours of receipt. The Contractor shall also meet or exceed paper claims turnaround requirements (data entered and adjudicated) within 3 Business Days of receipt.

46.31.3. Requirement Stage: All Contract Stages

46.32. Reference #2428: Claims/ encounters shall be identified, adjusted and re-processed, using the information that was current for the date of service at the time of processing the claim /encounter.

46.32.1. Contractor Approach: Contractor shall include information that was current for the dates of service at the time of processing the claim /encounter. The PBMS shall maintain and display historical reference data.

46.32.2. Requirement Stage: All Contract Stages

46.33. Reference #2429: Provide detail and summary reporting on paid, adjusted, or denied claims/ encounters that are identified through claim edits to the Department.

46.33.1. Contractor Approach: Contractor shall provide detail and summary reporting claims/encounters that are identified through claim edits to the Department weekly. The PBMS shall be configured per the defined requirements of the Department for flagging, re-pricing, and denying claims. Contractor shall provide a claims and encounter extract in the NCPDP Post Adjudication standard format to the MMIS as required and per a schedule and/or file layout determined during implementation.

46.33.2. Requirement Stage: All Contract Stages

46.34. Reference #2430: Adjudicate claims in accordance with Department policies and federal requirements.

46.34.1. Contractor Approach: The Contractor shall adjudicate claims in accordance with Department policies and federal requirements. The PBMS shall be highly configurable. The Contractor shall be able to make rapid adjustments in response to the changing policies and federal requirements, including formulary design, therapy limits, lock-ins, and other policy changes, via user configuration. The PBMS shall allow authorized business users to make metadata changes that support the needs of the Department to administer POS and batch claims processing in accordance with state legislation and policy and federal rules.

46.34.2. Requirement Stage: All Contract Stages

46.35. Reference #2431: Provide the ability to identify, edit and adjudicate claims/ encounters for services carved out of a managed care contract as a fee-for-service claim such as services for MC Pharmacy.

46.35.1. Contractor Approach: The Contractor shall be able to identify, edit, and adjudicate claims/encounters for carved out services according to Department specifications or requirements.

46.35.2. Requirement Stage: All Contract Stages

46.36. Reference #2432: Process claims/ encounters against defined services and policy and payment parameters within the Pharmacy Benefit Plan for each Pharmacy Benefit Plan.

46.36.1. Contractor Approach: Contractor shall process claims/encounters against defined services and policy and payment parameters within the Pharmacy Benefit Plan for each Pharmacy Benefit Plan. Contractor shall make determinations for payment in accordance with the applicable provisions in accordance with the Department Pharmacy Benefit Plan.

46.36.2. Requirement Stage: All Contract Stages

46.37. Reference #2433: Provide the ability to perform adjudication for individual claims/ encounters and batch claims/ encounters once received into the PBMS.

46.37.1. Contractor Approach: Contractor shall perform adjudication for individual claims/encounters and batch claims / encounters once received into the PBMS.

46.37.2. Requirement Stage: All Contract Stages

46.38. Reference #2434: Provide the ability to post edits and deny claims/ encounters from the same provider who is billing more than once for the same drug, client, and/ or the same claim.

46.38.1. Contractor Approach: Contractor shall post edits and deny claims/ encounters from the same provider billing more than once for the same drug, member, and/ or the same claim.

46.38.2. Requirement Stage: All Contract Stages

46.39. Reference #2435: Provide the ability to post edits and deny claims/ encounters from different providers who are billing separately for a drug for the same client.

46.39.1. Contractor Approach: Contractor shall post edits and deny claims/ encounters from different providers billing separately for a drug for the same member.

46.39.2. Requirement Stage: All Contract Stages

46.40. Reference #2436: Provide the ability to process, verify, and adjudicate mass adjustments for all paid and denied claims/ encounters and zero pays.

46.40.1. Contractor Approach: Contractor shall process, verify, and adjudicate mass adjustments for all paid and denied claims/encounters and zero pays. The PBMS shall provide mass adjustment functionality within the claim adjudication system.

46.40.2. Requirement Stage: All Contract Stages

46.41. Reference #2437: Provide parameter-driven multi-selection criteria for mass adjustment processing.

46.41.1. Contractor Approach: Contractor shall provide parameter-driven mass claims adjustment search are available for review and selection or de-selection prior to executing the resubmission or adjustment. Authorized users shall be able to select multiple clients, providers and/or Rx numbers when setting up mass adjustment jobs.

46.41.2. Requirement Stage: All Contract Stages

46.42. Reference #2438: Provide the ability to exclude claims/ encounters from mass adjustments that have zero impact to a payment.

46.42.1. Contractor Approach: Contractor shall provide the ability to exclude claims/encounters from mass claim adjustment job that have zero impact to a payment.

46.42.2. Requirement Stage: All Contract Stages

46.43. Reference #2439: Provide the ability to create a financial transaction for PBMS generated claims/ encounters through the Core MMIS and Supporting Services for payment.

46.43.1. Contractor Approach: Contractor shall provide PBMS claims/encounters data to the MMIS for payment in a format as directed by the Department.

46.43.2. Requirement Stage: All Contract Stages

46.44. Reference #2440: Provide the ability to perform the claim reconsideration process electronically so that claims and attachments are submitted electronically and connected in the PBMS.

46.44.1. The Contractor shall propose a solution that will work with the Department's system.

46.44.2. Contractor Approach: Contractor shall provide the ability to perform claim reconsiderations electronically. Reconsiderations will come in through Contractor's Pharmacy Call Center Services as a Claim Reconsideration Request. The request and the accompanying paper documentation (e.g. PCF-2, eligibility information, clinical information, etc.) will be imaged and retained and the request will be entered into the PBMS. These requests shall be routed via workflow to Contractor's Pharmacy Call Center Manager who will be responsible for review and disposition of the request, according to Department direction/policy. If required, the request shall be queued to the Department for review and decision. The Department will notify the Pharmacy Call Center Manager or Pharmacist of the next steps. If denied, contractor shall notify the submitter (who can then escalate to an appeal). If approved, contractor shall configure the PBMS to allow claim(s) to process and adjudicate and the submitter is notified. The Contractor shall partner with the Department during Discovery and Requirements Validation/Requirements Elicitation Phase of the Implementation Contract Stage to further understand the current process and set up a process that facilitates smooth handling of reconsideration requests.

46.44.3. Requirement Stage: All Contract Stages

46.45. Reference #2441: Provide the ability to adjust, process and/ or price Medicaid/ Medicare dual eligible claims/ encounters in accordance with Medicare guidelines. This includes claims/ encounters for clients who are in Medicare Managed Care, including Part C.

46.45.1. The Contractor shall only apply this ability to any Durable Medical Equipment (DME) supplies or physician administered drugs that are billed through the PBMS.

46.45.2. Contractor Approach: Contractor shall adjust, process and price Medicaid/Medicare dual-eligible claims and encounters, for durable medical equipment (DME) supplies and physician administered drugs only, within Medicare and the Department's guidelines, including members who are in Medicare Managed Care, including Part C.

46.45.3. Requirement Stage: All Contract Stages

46.46. Reference #2442: Provide the ability to adjudicate claims/ encounters based on national standard adjustment reason codes and remark codes from third parties where Medicaid is not the primary payer.

46.46.1. Contractor Approach: Contractor shall provide the ability to adjudicate claims/ encounters based on national standards. The PBMS shall be configured to support claims and encounter adjudication for valid values based on the Department's specific policy. PBMS user configurable functionality shall be where all online pharmacy claim and encounter correction and adjustment is performed in addition to it being the

solution in which all edits and audits are maintained and performed for paper and POS claims submitted by providers and batch encounter claims submitted by the managed care organizations.

46.46.2. Requirement Stage: All Contract Stages

46.47. Reference #2443: Provide the ability for authorized PBMS users to view the pricing methodology and calculations used to process each claim/ encounter.

46.47.1. The Contractor shall track the rate applied to a claim and the rate source and then document them on the claim record.

46.47.2. Contractor Approach: The Contractor shall track the rate applied to a claim and the rate source and document them on the claim record in the claim system. The Contractor shall provide the ability for authorized PBMS users to view pricing methodology and calculations used to price the claim/encounter. The PBMS shall be the financial rules engine where all claims data received are processed through the table driven algorithms to determine both the disposition and price of the claim and viewable on-line.

46.47.3. Requirement Stage: All Contract Stages

46.48. Reference #2444: Calculate and set Medicaid co-pays by Pharmacy Benefit Plan and by client eligibility.

46.48.1. Contractor Approach: Contractor shall calculate Medicaid co-pays by Pharmacy Benefit Plan and by client eligibility. The PBMS pricing module shall take into account all program rules, including but not limited to, existence of co-pays, deductibles and other client financial responsibilities.

46.48.2. Requirement Stage: All Contract Stages

46.49. Reference #2445: Provide the ability to price claims/ encounters irrespective of submission media type.

46.49.1. Contractor Approach: Contractor shall price claims/ encounters irrespective of submission media type.

46.49.2. Requirement Stage: All Contract Stages

46.50. Reference #2446: Manage current and historical reference data so that updates do not overlay and historical information is maintained and made accessible.

46.50.1. The Contractor shall ensure that:

46.50.1.1. Only the most current reference file information is used in business functions, including but not limited to, processing claims/ encounters and producing reports.

46.50.1.2. It possesses the capability of being date-specific and allows for multiple date periods to remain accessible for business functions.

46.50.2. Contractor Approach: Contractor shall manage current and historical reference data so that updates do not overlay historical information. Contractor shall establish procedures to process and store reference files such as drug, enrollment, provider and practitioner groups. These reference files shall support business functions for claims adjudication. All updated data shall be immediately utilized to support the accurate and timely disposition of pharmacy claims and encounters processing.

46.50.3. Requirement Stage: All Contract Stages

46.51. Reference #2447: Use co-insurance, co-pay and deductibles from third parties at the detail level for detail oriented claims/ encounters.

46.51.1. Contractor Approach: Contractor shall use co-insurance, co-pay and deductibles from third parties at the detail level for detail oriented claims/encounters. Contractor shall use patient financial responsibilities amounts as deductions to calculate the final payment amount.

46.51.2. Requirement Stage: All Contract Stages

46.52. Reference #2448: Limit payment for drugs to those described within the Pharmacy Benefit Plan and shall deny claims/ encounters exceeding dollar or utilization limits established in the Pharmacy Benefits Plan.

46.52.1. Contractor Approach: Contractor shall limit payment for drugs to those described within the Pharmacy Benefit Plan and shall deny claims/encounters exceeding dollar or utilization limits established in the Pharmacy Benefit Plan. Contractor shall provide a highly configurable rules engine that supports user configuration to define cost ceiling and utilization limit rules that identify limits.

46.52.2. Requirement Stage: All Contract Stages

46.53. Reference #2449: Provide the ability to categorize and separate claims from encounters in the PBMS.

46.53.1. Contractor Approach: The Contractor shall categorize and separate claims from encounters in the PBMS. The PBMS shall store each claim and encounter as a separate transaction regardless of the media type.

46.53.2. Requirement Stage: All Contract Stages

46.54. Reference #2450: Provide the ability to store and identify claims/ encounters as discrete data sets.

46.54.1. Contractor Approach: The PBMS shall store and identify each claim and encounter as a separate transaction regardless of the media type.

46.54.2. Requirement Stage: All Contract Stages

46.55. Reference #2451: Allow batch process and online process of encounter corrections, replacements and voids.

46.55.1. Contractor Approach: Contractor shall allow batch process and online processing of encounter corrections, replacements and voids. The PBMS shall support batch and online processing of encounter corrections, replacements and voids in the NCPDP Telecommunication Standard.

46.55.2. Requirement Stage: All Contract Stages

46.56. Reference #2452: Provide the capability to capture benefits used in a managed care plan and then apply those services to the benefit limits when a client returns to FFS.

46.56.1. Contractor Approach: Contractor shall provide the capability to capture benefits used in managed care plan and then apply those services to the benefit limits when a client

returns to FFS. The Contractor shall maintain and apply benefits, such as quantity dispensed, related to encounter claims so that they may be used in the event that a client returns to FFS.

46.56.2. Requirement Stage: All Contract Stages

46.57. Reference #2453: Provide the ability to store, maintain and use Department defined reimbursement methodologies and sources in claims/encounters processing.

46.57.1. Contractor Approach: Contractor shall provide the ability to store, maintain and use Department defined reimbursement methodologies and sources in claims/encounters processing. The PBMS shall provide multiple configuration options to support the Department's reimbursement methodologies.

46.57.2. Requirement Stage: All Contract Stages

46.58. Reference #2454: Provide the ability for providers to report client payments on their claims/ encounters such as copays, co-insurance and deductibles.

46.58.1. Contractor Approach: Contractor shall report client payments on claims/encounters such as copays, co-insurance and deductibles. Contractor shall accept and apply client financial responsibility amounts, as reported on the claim/encounter, in the pricing algorithm to determine the Department's final allowed amount.

46.58.2. Requirement Stage: All Contract Stages

46.59. Reference #2455: Perform quality control procedures to screen and capture electronic images, date-stamp, Julian date, assign unique control numbers and batch hardcopy claim forms and attachments, adjustment/ reconsiderations and updated documents.

46.59.1. The Contractor shall adhere to the Deliverable submission, review, and approval process as described and approved by the Department within the QA Control/ Quality Management Plan.

46.59.2. Contractor Approach: Contractor shall adhere to the Department's Deliverable submission, review, and approval process as described and approved by the Department within the QA Control / Quality Management Plan. The Contractor shall perform the quality control procedures as defined by the Department.

46.59.3. Requirement Stage: All Contract Stages

46.60. Reference #2456: Utilize quality and validation procedures to ensure accuracy of the information from paper claims/ encounters and attachments entered into the PBMS and validate data entry before it is adjudicated.

46.60.1. The Contractor shall adhere to the Deliverable submission, review, and approval process as described and approved by the Department within the QA Control/ Quality Management Plan.

46.60.2. Contractor Approach: Contractor shall adhere to the Deliverable submission, review, and approval process approved by the Department within the QA Control / Quality Management Plan. Contractor shall utilize quality and validation procedures to ensure accuracy of information from paper claims/encounters and attachments entered into the PBMS and validate data entry before final adjudication.

46.60.3. Requirement Stage: All Contract Stages

46.61. Reference #2457: Provide the ability to capture TPL health insurance coverage provided by other contractors and match information to clients.

46.61.1. Contractor Approach: Contractor shall provide the ability to capture TPL health insurance coverage provided by other contractors and match information to clients. The PBMS shall provide agile and robust TPL cost avoidance functionality within the claims adjudication system. Through a batch process, the Contractor shall be able to submit claims/encounters to other contractors and receive information back to cost avoid prospectively and accept claim adjustments.

46.61.2. Requirement Stage: All Contract Stages

46.62. Reference #2458: Provide the ability to share TPL information with pharmacies.

46.62.1. Contractor Approach: Contractor shall provide TPL information with pharmacies in the claim adjudication process. The PBMS shall provide TPL information from the client's enrollment record. The PBMS shall edit all claims for the presence of TPL, using data on the member's enrollment record, as well as editing for any voluntary information submitted that is not yet available on the enrollment files. The PBMS shall fully support on-line coordination of benefits utilizing the NCPDP v.D.0 COB segment and data elements. If a member has verified other insurance coverage, the claim shall deny NCPDP 41 - Submit Bill to Other Processor or Primary Payer, when the incoming claim does not contain the COB segment or if the data submitted on the incoming claim do not match and are not all-inclusive of the information existing on the member's enrollment record. If a third party exists, the claim shall be rejected with an appropriate message and client TPL detail as provided on the client's enrollment record.

46.62.2. Requirement Stage: All Contract Stages

46.63. Reference #2459: Alert providers when billing a claim for a client that has TPL coverage.

46.63.1. Contractor Approach: Contractor shall provide TPL information with pharmacies in the claim adjudication process. The PBMS shall provide TPL information from the client's enrollment record. The PBMS shall edit all claims for the presence of TPL, using data on the member's enrollment record, as well as editing for any voluntary information submitted that is not yet available on the enrollment files. The PBMS shall fully support on-line coordination of benefits utilizing the NCPDP v.D.0 COB segment and data elements. If a member has verified other insurance coverage, the claim shall deny NCPDP 41 - Submit Bill to Other Processor or Primary Payer, when the incoming claim does not contain the COB segment or if the data submitted on the incoming claim do not match and are not all-inclusive of the information existing on the member's enrollment record. If a third party exists, the claim shall be rejected with an appropriate message and client TPL detail as provided on the client's enrollment record.

46.63.2. Requirement Stage: All Contract Stages

46.64. Reference #2460: Accept and process claims/ encounters adjustments from Medicare enrolled clients.

46.64.1. This only applies to DME supplies and physician administered drugs.

46.64.2. Contractor Approach: Contractor shall accept and process claims/ encounters adjustments from Medicare enrolled clients. Contractor shall maintain data that identifies members who are dually eligible for Medicare. Contractor shall process and price Medicaid/Medicare dual-eligible claims and encounters, for DME supplies and physician administered drugs only, within Medicare and the Department's guidelines, including members enrolled in Parts D and C.

46.64.3. Requirement Stage: All Contract Stages

46.65. Reference #2461: Accept and process claims/ encounters adjustments from third parties such as primary insurance companies.

46.65.1. Contractor Approach: Contractor shall accept and process claims/encounters adjustments from third parties such as primary insurance companies as directed by the Department. The Contractor shall reprocess or demonstrate that an adjustment occurred on identified claims/encounters.

46.65.2. Requirement Stage: All Contract Stages

46.66. Reference #2462: Provide the ability to apply, track and document recovered or recoverable monies to the appropriate claims/ encounters.

46.66.1. Contractor Approach: Contractor shall provide the ability to apply, track and document recovered monies to the appropriate claims / encounters at the level corresponding to the allowed charge. Within the PBMS, Code Table Maintenance functionality business users shall be able to add specific Recovery Codes and Descriptions (e.g. TPL, Date of Death) to tag and identify claims that have financial recovery performed.

46.66.2. Requirement Stage: All Contract Stages

46.67. Reference #2463: Automate TPL recovery data to minimize paper transactions. PBMS shall support the upload of recovered money and automated association of those funds to claims.

46.67.1. Contractor Approach: Contractor shall automate TPL recovery processing to minimize paper transactions. The PBMS shall support the upload of recovered money and provide an automated association of funds to claims at the service level.

46.67.2. Requirement Stage: All Contract Stages

46.68. Reference #2464: Provide the ability to assign clients to providers within a new Pharmacy Benefit Plan as a part of the Client Over-Utilization Program (COUP) program so that clients can only receive benefits from specific pharmacies, prescribers or combinations of the two (2).

46.68.1. Contractor Approach: Contractor shall assign clients to providers within a Pharmacy Benefit Plan as a part of the COUP program so that Clients can only receive benefits from specific pharmacies, prescribers or combinations of the two (2). The PBMS shall be designed to support clinical efficiency and the configuration of edits and rules based on client designation, including lock-in, or any other designation as directed by the Department. The PBMS shall support the ability to maintain member restriction data including date parameters, provider, and pharmacy information to support claims processing functions. The PBMS shall utilize data stored in the client enrollment file,

or additional data provided by the Department, to perform verification and categorize member groupings and make systematic decisions based on direction by the Department.

46.68.2. Requirement Stage: All Contract Stages

46.69. Reference #2465: Provide the ability to enroll and identify a Managed Care Organization's provider network information separately and to affiliate with the Managed Care Organization.

46.69.1. Contractor Approach: Contractor shall provide the ability to identify and assign a Managed Care Organization's provider network information and to affiliate with the Managed Care Organization.

46.69.2. Requirement Stage: All Contract Stages

46.70. Reference #2466: Provide the ability to adjudicate claims based on provider type and specialty data from the MMIS such as only allowing mental health medications to be prescribed by a psychiatrist.

46.70.1. Contractor Approach: Contractor shall adjudicate claims based on provider type and provider specialty data received from the MMIS. The PBMS shall provide robust configuration options.

46.70.2. Requirement Stage: All Contract Stages

46.71. Reference #2467: Edit claims/ encounters based on presence of prior authorization.

46.71.1. Contractor Approach: Contractor shall edit claims/encounters based on presence of PA. The PBMS shall be an integrated POS adjudication system that includes its own PA and ProDUR modules to eliminate the need to communicate with secondary systems during the POS process, thus improving response time to the provider. When an encounter is adjudicated, any PA edit shall be pay and report using FFS edits.

46.71.2. Requirement Stage: All Contract Stages

47. ENCOUNTER CLAIMS

47.1. Reference #2468: Allow the Department to perform manual enrollment/ disenrollment functions so that business operations are not interrupted by PBMS limitations.

47.1.1. Contractor Approach: Contractor shall allow authorized PBMS users to manually enroll/disenroll clients into MCOs and Pharmacy Benefit Plans.

47.1.2. Requirement Stage: All Contract Stages

47.2. Reference #2469: Support accurate and timely automatic or choice-based enrollment of clients into a Pharmacy Benefit Plan. PBMS generates error report when a client is incorrectly enrolled.

47.2.1. The Contractor shall resolve any enrollment issues within their control within 48 hours.

47.2.2. Contractor Approach: Contractor shall integrate closely with the MMIS enrollment system and maintain client eligibility information from the MMIS necessary to adjudicate claims, process prior approvals, and calculate cost sharing. Contractor shall accept client eligibility information in the Standard NCPDP 834 Enrollment transaction

or use a State defined format if necessary. Contractor shall have the ability to receive client updates at 15-minute intervals or once daily depending on the Department's need. The Contractor shall correct any errors in the PBMS within the Contractor's control resulting from load exceptions from the MMIS.

47.2.3. Requirement Stage: All Contract Stages

47.3. Reference #2470: Accept client enrollment and disenrollment data from the MMIS and assign to the correct Pharmacy Benefit Plan.

47.3.1. The Contractor shall resolve any enrollment issues within their control within 48 hours.

47.3.2. Contractor Approach: Contractor shall integrate closely with the MMIS enrollment system and maintain client eligibility information from the MMIS necessary to adjudicate claims, process prior approvals, and calculate cost sharing. Contractor shall accept client eligibility information in the Standard NCPDP 834 Enrollment transaction or use a State defined format if necessary. Contractor shall have the ability to receive client updates at 15-minute intervals or once daily depending on the Department's need. The Contractor shall correct any errors in the PBMS within the Contractor's control resulting from load exceptions from the MMIS.

47.3.3. Requirement Stage: All Contract Stages

47.4. Reference #2471: Enroll clients into specified Pharmacy Benefit Plan according to criteria established by the Department

47.4.1. The Contractor shall resolve any enrollment issues within their control within 48 hours.

47.4.2. Contractor Approach: The Contractor shall accept client enrollment data from the MMIS and assign to the correct Pharmacy Benefit Plan based on attributes in the enrollment file from the MMIS based on the Department's criteria. Contractor shall resolve enrollment issues within their control within 48 hours.

47.4.3. Requirement Stage: All Contract Stages

47.5. Reference #2472: Allow for Configuration of hybrid, fee-for-service managed care models as a Pharmacy Benefit Plan, such as when certain drugs are carved out of a managed care model.

47.5.1. The Contractor shall resolve any enrollment issues within their control within 48 hours.

47.5.2. Contractor Approach: The Contractor shall support Configuration of hybrid fee-for service managed care model as a Pharmacy Benefit Plan, such as when certain drugs are carved out of a managed care model.

47.5.3. Requirement Stage: All Contract Stages

47.6. Reference #2473: Allow authorized PBMS users to manually enroll and disenroll a client into a Pharmacy Benefit Plan.

47.6.1. The Contractor shall resolve any enrollment issues within their control within 48 hours.

47.6.2. Contractor Approach: Contractor shall allow authorized PBMS users to manually enroll/disenroll clients into MCOs and Pharmacy Benefit Plans.

47.6.3. Requirement Stage: All Contract Stages

47.7. Reference #2474: Maintain current and historical records of Pharmacy benefit assignment(s) for clients.

47.7.1. Contractor Approach: The Contractor shall maintain current and historical records of Pharmacy benefit assignment(s) for clients.

47.7.2. Requirement Stage: All Contract Stages

47.8. Reference #2475: Performs client copay reset processing annually.

47.8.1. The PBMS shall track the percentage of the client's or family's income spent on copays.

47.8.2. The PBMS shall be able to 'turn off' the client's copay requirement when the amount paid reaches Department defined limitations for a specified time frame.

47.8.3. The Department will provide the Client or Family federal poverty level (FPL) or income in the eligibility interface to facilitate this process.

47.8.4. Contractor Approach: Contractor shall reset copayment threshold amounts annually, as directed by the Department. Contractor shall accumulate for tracking client's or family's income spent on copays.

47.8.5. Requirement Stage: All Contract Stages

47.9. Reference #2476: Provide the ability to uniquely identify the Managed Care Organization associated with an encounter.

47.9.1. Contractor Approach: Contractor shall provide the ability to uniquely identify the Managed Care Organization associated with an encounter. The Contractor shall assign the Managed Care entity a unique batch identifier for encounter processing. The PBMS shall be able to immediately identify the Managed Care Organization by this identifier.

47.9.2. Requirement Stage: All Contract Stages

47.10. Reference #2477: Allow authorized PBMS users to manually enroll Colorado Medical Assistance program clients whose eligibility is not submitted or received through CBMS.

47.10.1. Contractor Approach: Contractor shall grant authorized PBMS users access to enroll Colorado Medicaid Assistance program clients whose eligibility is not submitted or received. Manual eligibility additions and modifications shall be able to be performed by authorized PBMS users.

47.10.2. Requirement Stage: All Contract Stages

47.11. Reference #2478: Capture providers and associated Encounter Data received from the managed care plan with each provider.

47.11.1. Contractor Approach: Contractor shall capture provider and encounter data received from the managed care plan with each provider as shown on the encounter.

47.11.2. Requirement Stage: All Contract Stages

48. STATE REIMBURSEMENT METHODOLOGIES

48.1. Reference #2479: Maintain all historical and current pricing methodologies as established by the Department.

48.1.1. Contractor Approach: Contractor shall maintain historical and current pricing methodologies as established by the Department. The historical information shall contain the effective and termination dates for the pricing methodology. Current information shall contain the effective date for the pricing methodology.

48.1.2. Requirement Stage: All Contract Stages

48.2. Reference #2480: Provide the ability to receive pricing information via an extract or interface file from various sources, including 3rd party vendors, CMS and the Department, and input into PBMS.

48.2.1. Contractor Approach: Contractor shall provide the ability to receive pricing information via an extract or interface from various sources, including 3rd party vendors, CMS and the Department, and input into PBMS. The PBMS shall have the flexibility to utilize any commercially available and/or provided proprietary pricing information during reimbursement calculation, through the Change Management Process if changes to the source require a change to the PBMS.

48.2.2. Requirement Stage: All Contract Stages

48.3. Reference #2481: Provide a configurable system to allow for updates and changes to rates within the various pricing methodologies and by provider type and /or plan type.

48.3.1. Contractor Approach: Contractor shall provide a configurable rules engine to allow for updates and changes to rates within pricing methodologies. The PBMS shall allow for rates within various pricing methodologies and by provider type and/or plan type to support the claim processing.

48.3.2. Requirement Stage: All Contract Stages

48.4. Reference #2482: Create date-sensitive modifications to the reimbursement rates as directed by the Department.

48.4.1. Contractor Approach: Contractor shall create date sensitive modifications to the reimbursement rates as directed by the Department. The historical records shall contain the effective and termination dates for the reimbursement rates. Current records shall contain the effective date for the reimbursement rates.

48.4.2. Requirement Stage: All Contract Stages

48.5. Reference #2483: Price claims based on reimbursement methodology criteria and date specifications set by the Department.

48.5.1. Contractor Approach: Contractor shall price claims based on defined reimbursement methodology criteria set by the Department. The PBMS shall allow for pricing algorithms to be configured at the plan, provider group, member type, drug, and/or MCO level. The PBMS shall have the ability to support different pricing methodologies based on characteristics of the provider and/or member type such as benefit package, age, Indian Health Services Pharmacies and long-term-care (LTC) among others.

48.5.2. Requirement Stage: All Contract Stages

48.6. Reference #2484: Maintain all historical and current dispensing fees as established by the Department.

48.6.1. Contractor Approach: Contractor shall maintain all historical and current dispensing fees as established by the Department. Contractor shall maintain all active, inactive, and logically deleted adjudication rules including rules for dispense fee. The historical records shall contain the effective and termination dates for the dispensing fees. Current records shall contain the effective date for the dispensing fees.

48.6.2. Requirement Stage: All Contract Stages

48.7. Reference #2485: Provide an easily configurable system to allow for updates and changes to dispensing fees by provider type, plan type and total prescription volume.

48.7.1. Contractor Approach: Contractor shall provide its easily configurable rules engine to support updates and modify dispensing fees by provider type, plan type and total prescription volume. All rules in the PBMS shall be configured with an effective and termination date.

48.7.2. Requirement Stage: All Contract Stages

48.8. Reference #2486: Create date-sensitive modifications to the dispensing fees as directed by the Department.

48.8.1. Contractor Approach: Contractor shall create date-sensitive modifications to the dispensing fees as directed by the Department. The historical records shall contain the effective and termination dates for the dispensing fees. Current records shall contain the effective date for the dispensing fees.

48.8.2. Requirement Stage: All Contract Stages

48.9. Reference #2487: Price claims using the dispensing fee criteria and date specifications set by the Department.

48.9.1. Contractor Approach: Contractor shall price claims using the dispensing fee criteria and date specifications set by the Department. Contractor shall use rules that are in effect on that date of service to adjudicate claims.

48.9.2. Requirement Stage: All Contract Stages

49. PHARMACY PRIOR AUTHORIZATION

49.1. Reference #2488: Provide an auto-assigned unique, non-duplicated PAR number for tracking throughout the life of the PAR. This PAR number shall be used in claim/ encounter processing to validate the services and shall be recorded on the claim record.

49.1.1. The Contractor shall ensure that PAR numbers remain consistent between PBMS and MMIS and/or BIDM, as directed by the Department.

49.1.2. Contractor Approach: Every PA entered in the system shall be assigned a unique “Rule ID” and if necessary this “Rule ID” shall be able to be viewed as a PA number and used in the claim submission process if passed to the prescriber and/or pharmacy at the time of PA approval. This “Rule ID” shall be able to have a one to many relationship with a claim if the length of the PA is such that the member would fill multiple claims for the same medication throughout the life of the PA (e.g. a one-year PA for a mediation that is filled at the pharmacy on a monthly basis would result in a one PA “Rule ID” to many claims situation). It shall also be possible to have a one claim to many PA “Rule

ID" situation (e.g., an incoming claim required an authorization to dispense for any member, but also has quantity limits which a particular member is authorized to exceed). This situation would result in a single claim with multiple PA "Rule IDs" because each of these situations is a distinct edit type that would require a distinct PA and thus have multiple "Rule IDs" that the claim would use to adjudicated. The Contractor shall transmit this "Rule ID" to the MMIS and/or BIDM, as directed by the Department.

49.1.3. Requirement Stage: All Contract Stages

49.2. Reference #2489: Provide the ability to accept, store and edit PARs, including the ability to automatically and manually edit PARs.

49.2.1. Contractor Approach: The PBMS shall have fully integrated AutoPA feature that streamlines the PA process for the provider and prescriber through the use of automated decision-making based on established and approved clinical rules and edits within the processing engine. AutoPA shall use information submitted on the claim and stored in the member profile (past drug use, diagnosis codes, etc) to determine the appropriate disposition of the claim guided by Department-approved criteria. Contractor's solution shall eliminate most manual entry of PA records for authorized users, based on the configurable Auto PA capability.

49.2.2. In case a claim requires manual prior authorization by design, or because it failed POS AutoPA rules, the prescriber shall be able to contact the Pharmacy Support Center. The Contractor shall accept, store and edit PARs via phone, fax, web or other mutually agreed PA submission methodologies. Authorized users shall be able to manually apply overrides based on exceptions for payment. The PBMS shall include a sophisticated clinical initiative feature which provides intuitive groupings of information (e.g., all associated edits — including linkage to internal error codes — and the drug classification level for authorization). This feature, combined with the auto-population of data in a pre-defined "template," shall facilitate the reviewer's completion of the prior authorization record. Information from a denied claim (e.g., member ID, name, group and plan, provider and prescriber ID, submitted drug code, drug quantity and days' supply, and date of service) shall be automatically populated on a template that is designed for the specific initiative associated with the prior authorization condition. This shall ensure that any/all edits necessary to override the prior authorization requirement are addressed via the completion of a single prior authorization record. For example, a complex prior authorization condition may require an override for medical necessity, quantity, and days-supply. The system shall be designed to return a template to the agent that includes all of the elements that must be completed.

49.2.3. Requirement Stage: All Contract Stages

49.3. Reference #2490: Identify and reject duplicate PARs.

49.3.1. Contractor Approach: The Contractor shall reject the request and notify the provider when a duplicate PAR is submitted or is not necessary. The PBMS shall have built-in hierarchical rules and system checks to ensure that only one PA record exists for the requested product.

49.3.2. Requirement Stage: All Contract Stages

49.4. Reference #2491: Provide the ability for authorized PBMS users to search and view prior authorizations by selected criteria such as provider, client, PAR type and drug information in the PBMS.

49.4.1. Contractor Approach: The Contractor shall allow authorized users to search and view prior authorizations by selected criteria.

49.4.2. Requirement Stage: All Contract Stages

49.5. Reference #2492: Provide the ability to link and view multiple PARs to a client record.

49.5.1. Contractor Approach: The PBMS shall provide the ability to maintain multiple authorizations on drug products for clients related to preferred or non-preferred status, clinical limitation (both quantity and fiscal). When multiple edits or authorizations apply to a product, each shall be met for a submitted claim to reach an approved or paid status. All PARs associated with a client record shall be linked and viewable through the PBMS.

49.5.2. Requirement Stage: All Contract Stages

49.6. Reference #2493: Provide the ability to produce notices to clients and providers regarding PARs.

49.6.1. Contractor Approach: Standard notice generation, such as client and provider prior authorization approval and denial letters, shall be produced for provider-initiated PARs using data contained within the PBMS. These notices shall be able to be created with variable text as needed.

49.6.2. PBMS users shall also have the ability to create a facsimile reply notice using the Department's template, for prior authorization requests received via facsimile, and communicate information necessary to providers either through standard or free-form text.

49.6.3. Requirement Stage: All Contract Stages

49.7. Reference #2494: Maintain PAR notifications and store all data used to populate the notification.

49.7.1. Contractor Approach: The PBMS shall document all applicable details related to a PA request, including denial reason. This detail shall allow for specific information to be included in notices generated for clients and providers.

49.7.2. Requirement Stage: All Contract Stages

49.8. Reference #2495: Provide the ability to update notification letters regarding PAR determinations when business rules are updated, such as when changing denial reasons.

49.8.1. Contractor Approach: The Contractor shall update PAR notifications to clients and providers when business rules are updated, based on direction from the Department and as specified through the Change Management Process.

49.8.2. Requirement Stage: All Contract Stages

50. PRO-DUR

50.1. Reference #2496: Provide easily configurable Pro-DUR edits based on Department and CMS standards.

50.1.1. Contractor Approach: Contractor shall provide configurable ProDUR edits based on Department and CMS standards.

50.1.2. Requirement Stage: All Contract Stages

50.2. Reference #2497: Ensure Pro-DUR edits are applied to claims and any edits that post are reported back to the submitting pharmacy.

50.2.1. Contractor Approach: Contractor shall ensure ProDUR edits are applied to claims and any edits that post are reported back to the submitting pharmacy.

50.2.2. Requirement Stage: All Contract Stages

50.3. Reference #2498: Ensure claim line level data, related to Pro-DUR edits, is transferred for storage to the BIDM.

50.3.1. Contractor Approach: Contractor shall ensure claim level data related to ProDUR edits, including claim/encounter pay and report DUR interventions, is transferred to the MMIS and/or BIDM, as directed by the Department.

50.3.2. Requirement Stage: All Contract Stages

51. DRUG REBATE SYSTEM

51.1. Reference #2499: Automate the transfer/ tracking of rebate payments from PBMS to the Colorado Operations Resource Engine (CORE).

51.1.1. Contractor Approach: The Contractor shall work with the Department to set up a lockbox to receive payments and pass on copies to Contractor.

51.1.1.1. Cognos reports shall be available for CORE as needed. Contractor understands that drug rebate payments will be sent to a Financial Institution Lockbox owned and maintained by the Department. The Contractor shall accept interfaces from the lock box in order to automate the processing of rebate checks.

51.1.1.2. Contractor shall be prepared to accept read-only online access to drug rebate payments and shall work with the Department to ensure the drug rebate invoice is scannable and meets the lockbox provider’s specifications.

51.1.1.3. The Contractor shall then interface with the lock box or obtain other information from the Department to disposition the payments.

51.1.2. Requirement Stage: All Contract Stages

51.2. Reference #2500: Provide the ability for all values to be viewable and searchable by Department authorized users.

51.2.1. Contractor Approach: The Contractor shall provide secure access to authorized Department users to the rebate reporting tool where all financial and invoice data is available.

51.2.1.1. The Contractor shall produce a full suite of standard reports and shall have the capability to build necessary reports for the Department upon request.

51.2.1.2. Reports shall be parameter-driven for user flexibility.

51.2.1.3. Rebate reporting tool data shall be refreshed in real time, so many of the reports shall be able to be generated with "up to the minute" data. The Contractor's reporting tools shall allow users to configure personal settings and preferences enabling them to opt to be notified or receive a copy via email every time a new version of a report is refreshed or becomes available.

51.2.2. Requirement Stage: All Contract Stages

51.3. Reference #2501: The rebate rules and associated logic, as well as the values calculated as a result of the rules, shall be viewable through the PBMS rebate application.

51.3.1. Contractor Approach: The Contractor shall have rules in place, such as claims exclusions and quantity limits. The rules and associated logic, as well as the values calculated as a result of the rules, shall be viewable through the PBMS rebate application.

51.3.2. Requirement Stage: All Contract Stages

51.4. Reference #2502: Create and maintain on-line reports which allow users to choose from multiple pre-built defined parameters, singly or in combination, to generate user Customized results that help users monitor the daily operations of the Rebate System. Online reports shall include historical rebate data and the most current data.

51.4.1. Reports shall include, but are not limited to:

51.4.1.1. Account Receivable Summary by Manufacturer,

51.4.1.2. Dispute Amount.

51.4.1.3. Dispute Code.

51.4.1.4. Batch Total.

51.4.1.5. Check.

51.4.1.6. Claims Balancing.

51.4.2. Contractor Approach: The Contractor shall provide secure access to authorized state users to the rebate reporting tool where all financial and invoice data are available, both historical and current.

51.4.2.1. The Contractor shall have the capability to build necessary reports for the Department upon request. The Contractor shall provide the ability for the Department to independently modify parameters within reports based on report design.

51.4.2.2. The rebate reporting tools shall allow users to configure personal settings and preferences enabling them to opt to be notified or receive a copy via email every time a new version of a report is refreshed or becomes available.

51.4.3. Requirement Stage: All Contract Stages

51.5. Reference #2503: Provide the ability for alerts to indicate new reports.

51.5.1. Contractor Approach: The rebate reporting tools shall allow users to configure personal settings and preferences enabling them to opt to be notified via alerts or receive a copy via email every time a report is executed in production.

51.5.2. Requirement Stage: All Contract Stages

51.6. Reference #2504: Contractor shall accept and store data for physician administered drugs from the MMIS and/or BIDM, as directed by the Department for rebate processing.

51.6.1. Contractor Approach: The Contractor shall establish independent programs for the POS drug claims and physician administered drug claims and send invoices to manufacturers separately. This shall allow payments to be allocated independently as well. The Department shall be able to track and report on all the information as needed.

51.6.2. Requirement Stage: All Contract Stages

51.7. Reference #2505: Report all drug Rebate System data to the BIDM and the MMIS.

51.7.1. Contractor Approach: The Contractor shall perform automated data transfers for drug rebate information to other systems, such as MMIS or BIDM, as directed by the Department.

51.7.1.1. The Contractor shall provide all required drug rebate data to the MMIS and BIDM including all drug rebate related data from its system needed to produce the CMS 64 and other data agreed upon by the Parties.

51.7.2. Requirement Stage: All Contract Stages

51.8. Reference #2506: Provide the flexibility to automate the processing, depositing and reporting of drug rebate checks from drug manufacturers through a lockbox process. This should include at a minimum a scannable remittance document (invoice) that meets the lockbox service provider's specifications and the ability to receive lockbox files which can be uploaded and reported by the System. This process must be in compliance with State fiscal policy and procedures.

51.8.1. The Contractor shall use general accepted processes in their response strategy.

51.8.2. Contractor Approach: The Contractor will receive paper or electronic copies of payments from a lockbox service and shall manually enter that information into the rebate reporting system for reports to populate with the payment information.

51.8.2.1. The Department will provide payment information (checks and associated documentation) that manufacturers submit to the drug rebate lock box.

51.8.2.2. The Contractor shall produce reports and provide data, as appropriate, to the MMIS, BIDM and CMS and shall comply with all CMS reporting requirements in the Contract, including producing data for the CMS 64.9R quarterly report.

51.8.3. Requirement Stage: All Contract Stages

51.9. Reference #2507: Drug Rebate information shall be sent to and stored in the BIDM. This will happen via a direct interface with the BIDM, or through an interface with the MMIS.

51.9.1. Contractor Approach: The Contractor shall perform automated data transfers for drug rebate information to other systems, such as MMIS and/or BIDM, as directed by the Department.

51.9.1.1. The Contractor shall provide all required drug rebate data to the MMIS and BIDM including all drug rebate related data from its system needed to produce the CMS 64 and other data agreed upon by the Parties.

51.9.2. Requirement Stage: All Contract Stages

51.10. Reference #2508: URA data from CMS shall be captured and stored in PBMS. Calculate and apply any modifications needed when the quantity standards vary between the URA and the claims.

51.10.1. Contractor Approach: The Contractor shall utilize a rebate application to validate and support the load of the CMS manufacturer, rebate rate and rebate offset rate files.

51.10.1.1. These files shall be retrieved directly from the CMS Medicaid Drug Rebate (MDR) website.

51.10.1.2. The Contractor shall be an authorized agent which eliminates the need to establish a new FTP process so that the Department's file can be transferred to the Contractor on the Department's behalf.

51.10.2. Requirement Stage: All Contract Stages

51.11. Reference #2509: Store all data related to drug rebate processing, including historical data, in the PBMS with functionality to easily query and access the data.

51.11.1. Contractor Approach: The Contractor shall load, store, and provide reporting capability for all electronic historical, current, and future rebate related data. All paper historical rebate related data shall be securely stored and accessible.

51.11.2. Requirement Stage: All Contract Stages

52. PREFERRED DRUG LIST

52.1. Reference #2510: Create all PDL reports as specified by the Department.

52.1.1. Contractor Approach: The Contractor shall provide its standard suite of reports to the Department

52.1.1.1. The Contractor shall identify gaps in the established standard suite of reports during the requirements phase, and create additional PDL reports as specified by the Department.

52.1.2. Requirement Stage: All Contract Stages

52.2. Reference #2511: Provide average daily cost comparison for drugs within reviewed PDL classes in a quarterly report.

52.2.1. Contractor Approach: The Contractor provide a quarterly average daily cost comparison report, for drugs within a PDL class. The Contractor shall calculate the average daily cost as agreed to by the Parties.

52.2.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

52.3. Reference #2512: Make all system changes necessary to support the criteria for PDL processing.

52.3.1. Contractor Approach: The Contractor shall follow the standard Change Management Process for system changes to support the PDL.

52.3.1.1. The Contractor shall utilize the PBMS to support product assignments to PDL preferred and non-preferred status and any associated prior authorization criteria.

52.3.1.2. The PBMS shall provide the ability to manage clinical, operational, and PDL drug benefit configuration through PBMS functionality.

52.3.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

53. PHARMACY REFERENCE DATA MANAGEMENT

53.1. Reference #2513: Provide reference files containing all data required to provide validation and pricing verification during claims/ encounters processing for all approved claim/ encounters and reimbursement methodologies.

53.1.1. Contractor Approach: The PBMS shall serve as the repository for all reference data required to support the accurate and timely disposition of pharmacy claims. All files that are loaded as reference information shall be reviewed and validated for accuracy and timeliness. If a concern or issue is identified that questions the timing or accuracy of the file, it shall be immediately escalated for appropriate review and prompt resolution. The Contractor shall ensure all required data elements are transferred to the BIDM in compliance with the Contractor's licenses.

53.1.2. Requirement Stage: All Contract Stages

53.2. Reference #2514: Provide the ability to retrieve archived reference data.

53.2.1. Contractor Approach: All reference data shall be maintained on the PBMS throughout the term of the Contract. In the event data is archived for some reason, it shall be made available to authorized PBMS users.

53.2.2. Requirement Stage: All Contract Stages

53.3. Reference #2515: Perform quality control on all reference file updates to ensure the integrity of data.

53.3.1. Contractor Approach: The Contractor shall put overall quality management in place and perform quality control on all reference file updates to ensure the integrity of data. All files that are loaded as reference information shall be reviewed and validated for accuracy and timeliness. If a concern or issue is identified that questions the timing or accuracy of the file, it shall be immediately escalated for appropriate review and resolution. Load reports shall be available for review and analysis to ensure that records have been added or updated in a timely and accurate manner.

53.3.2. Requirement Stage: All Contract Stages

54. PROGRAM INTEGRITY

54.1. Reference #2516: Provide claim information that can be used for proving fraud and abuse cases in a legal setting. The Contractor shall store and make available original claim/ encounter information submitted by the provider and generate facsimile of the appropriate claim/ encounter format, on a claim-by-claim basis.

54.1.1. Contractor Approach: The Contractor shall store and make available original claim/ encounter information submitted by the provider and generate facsimile of the appropriate claim/ encounter format, on a claim-by-claim basis. The Contractor shall expeditiously respond to agency requests, claim/encounter-by-claim/encounter if necessary. Contractor shall gather claim-related data submitted by the pharmacy and extracted from data warehouse, including materials such as the original claim, reversals, and denials. Claim data shall be able to then be moved into the Contractor's PI case management system that stores case related claims, case notes, copies of pharmacy submitted documents, and member and prescriber data. Data shall also be able to be supplied and maintained if outside agencies such as, the Attorney General, Office of Inspector General, Medicaid Fraud Control Unit, or the Department's Special Investigations Unit makes requests.

54.1.2. Requirement Stage: All Contract Stages

54.2. Reference #2517: Provide the ability in the PBMS to identify claims/ encounters currently and previously subject to audit or recovery down to the line detail level.

54.2.1. Contractor Approach: The Contractor shall use the claim adjustment process to note the recovery type, such as placing a $0.00 claim recovery and the proper adjustment reason code to note that an item had been reviewed even if no action was taken. In the event that the data feed for this requires Configuration or Customization to accept, then this change shall occur through the Change Management Process.

54.2.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Stage

55. PHARMACY BENEFIT MANAGEMENT SYSTEM SUPPORT AND OPERATIONS

55.1. Reference #2518: Receive provider enrollment files from the Core MMIS and Supporting Services Contractor and enroll providers into the PBMS to support claims adjudication.

55.1.1. Contractor Approach: The Contractor shall use the standard NCPDP service provider file as a reference file in the PBMS for NPI numbers for pharmacy service providers, and a national prescriber file to support the business needs of the Department. The Contractor shall also load the MMIS prescriber and pharmacy provider information, including the NPI number, into PBMS for use in the adjudication process. The PBMS shall validate pharmacy provider and prescribing provider information received from the MMIS early in the adjudication process. If the submitted information does not pass the verification and validation checks, NCPDP reject messages shall be returned to the submitter with additional messaging identifying the issue in order to expedite a resolution.

55.1.2. Requirement Stage: All Contract Stages

55.2. Reference #2519: In conjunction with the Department, develop and maintain provider publication formats/ updates and content and provide this information to the Department or the MMIS, as directed by the Department, for publication.

55.2.1. Contractor Approach: The Contractor shall ensure that documentation meets rigorous standards for quality. The Contractors document management control processes shall govern the creation, review, approval, and publication of critical documents. Key areas of focus shall include templates, document storage and access, review, and approval.

The Contractor shall ensure materials are accurate, clear, and consistent. The Contractor shall work closely with the Department to create, update, maintain and store provider publications for the Department's PBMS. The documentation the Contractor creates shall comply with all readability and formatting requirements; and the Contractor shall provide this documentation to the Department or the MMIS, as directed by the Department for publishing once the Department approves the content.

55.2.2. Requirement Stage: All Contract Stages

55.3. Reference #2520: Provide authorized PBMS users online access to edit and publish all provider publications such as manuals, bulletins, billing instructions, notices and subsequent updates.

55.3.1. Contractor Approach: The Contractor shall provide authorized PBMS users online access to edit and publish all provider publications (e.g., manuals, bulletins, billing instructions, notices, and subsequent updates). All provider publications shall be archived in the document management system for ease of recovery.

55.3.2. Requirement Stage: All Contract Stages

55.4. Reference #2521: Archive historical provider publications in a searchable area accessible to the Department staff.

55.4.1. Contractor Approach: The Contractor shall maintain all historical provider publications in the shared document repository. This system shall be capable of providing document search functionality to the Department staff. The shared document repository shall provide secure storage of these artifacts and shall be accessible by authorized Department users.

55.4.2. Requirement Stage: All Contract Stages

55.5. Reference #2522: Support desktop mail merge functionality that allows authorized PBMS users to easily export PBMS information on clients and providers so that it can be merged into template letters and forms to communicate with clients, providers, and others as directed by the Department.

55.5.1. The Contractor shall ensure that this feature allows for the ability to export data to produce Custom letters or forms using a desktop application, such as Microsoft Word, outside of the PBMS letter generation solution.

55.5.2. Contractor Approach: The Contractor shall provide an enterprise solution which shall produce correspondence using templates created in Microsoft Word. Correspondence shall be produced when triggered by a configured event or as part of a workflow configured in the PBMS. The Contractor shall allow the Department to export information from the PBMS reporting solution into common formats, such as Microsoft excel, to facilitate mail merges.

55.5.3. Requirement Stage: All Contract Stages

55.6. Reference #2523: Provide the ability to target specific provider groups with communications taking into consideration the audience and timing, per Department requirements.

55.6.1. Contractor Approach: The Contractor shall utilize both the NCPDP service provider file for necessary demographic information for pharmacy providers (including NPI numbers, mailing addresses) and a national prescriber file for prescriber demographic information (including NPI numbers, mailing address). In addition, the Contractor shall load and utilize provider/prescriber files provided by the MMIS Contractor for additional demographic information (e.g. specialty indicators). Utilizing Department approved communications content developed by the Contractor, the Contractor shall use demographic data attributes available in these files (e.g. specialty indicators, taxonomy codes, mailing address) to provide provider specific targeted groups with communications per Department approved requirements.

55.6.1.1. The Contractor shall meet this requirement with the Contractor's enterprise solution, Correspondence Publisher.

55.6.2. Requirement Stage: All Contract Stages

55.7. Reference #2524: Establish and participate in weekly PBMS Operations status meetings with key Department personnel to discuss progress, issues, problems, and planning. The Contractor shall report on current operations status, progress on PBMS maintenance, claims/ encounters inventory balances, claims/ encounters backlogs, data entry backlog, and suspense file status, and modification activities separately. The Contractor shall be responsible for preparing and distributing a meeting agenda. The Contractor shall be responsible for preparing and distributing meeting minutes for Department review, and maintaining final approved agenda/ minutes.

55.7.1. The Contractor shall deliver the agenda to the Department no later than one (1) Business Day prior to the meeting for which the agenda was produced. The Contractor shall deliver all meeting minutes to the Department no later than three (3) Business Days following the meeting to which the minutes apply.

55.7.2. Contractor Approach: The Contractor shall establish Weekly Status meetings with the Department at a mutually agreeable time. A toll free secure phone number shall be provided by the Contractor for personnel located off site to access the call.

55.7.3. Contractor shall send out an agenda at least 24 hours in advance which contains the call time, phone number and the items for discussion.

55.7.3.1. During the meeting, a designated Contractor resource shall be responsible for taking meeting minutes on all topics brought up at the meeting,

55.7.4. Contractor shall create draft meeting minutes which contain the call date and time, list of meeting participants, and details regarding all of the topics discussed. The minutes shall be distributed via email message and any discrepancies are communicated to the author and the final version is distributed to all parties and stored in a document retrieval system for future reference.

55.7.5. Deliverable: PBMS Operations Status Meeting Agenda; PBMS Operations Status Meeting Minutes.

55.7.6. Deliverable Stage: PBMS Ongoing Operations and Enhancement Contract Stage

55.8. Reference #2525: Contractor shall provide monthly call center reports on telephonic communications with clients and providers that includes calls answered, length of calls, hold time, and abandoned calls.

55.8.1. Contractor Approach: The Contractor shall provide monthly call center telephone reports detailing information for both provider and customer calls. The Contractor shall report on data such as calls total number answered, average length of calls, hold time, and number of abandoned calls.

55.8.2. Deliverable: Monthly Call Center Report.

55.8.3. Deliverable Stage: All Contract Stages

55.9. Reference #2526: Coordinate PBMS and supporting systems-related interactions between the Department and other contractors required to manage and execute a process using the PBMS.

55.9.1. Contractor Approach: The Contractor shall make technical and business resources available to coordinate interactions between the Department and other contractors in order to manage and execute a process using the PBMS. Interactions may include such activities as walkthroughs of interface documentation, JAD sessions, educational meetings and structured design sessions.

55.9.2. Requirement Stage: All Contract Stages

55.10. Reference #2527: Maintain client records in the PBMS and provide response to provider inquiries on client claims, services, or benefits, as appropriate.

55.10.1. Contractor Approach: The Contractor shall provide a Pharmacy Support Center at which the primary responsibility shall be to assist pharmacy providers with a variety of inquiries. PSC staff shall be trained on information that shall allow them to educate providers and answer questions based on data elements used in successfully transmitting claims to the PBMS. In addition, the Contractor shall provide assistance with items, such as prior authorizations status, preferred drug list (PDL) questions, drug coverage, enrollment status, payment status, COB payer information, non-clinical inquiries about ProDUR messages, and policy and procedures information. The Contractor shall also field software vendor issues.

55.10.2. Requirement Stage: All Contract Stages

55.11. Reference #2528: Maintain the appropriate level of knowledgeable staff that are capable of testing, validating and documenting operational impacts of changes to the PBMS.

55.11.1. The Contractor shall maintain all staffing in accordance with the Resource Management Plan.

55.11.2. Contractor Approach: The Contractor shall provide quality assurance staff, as well as a staff of plan administrators in accordance with the Resource Management Plan. These two groups shall manage the design configuration, testing validation and documentation of modifications to the Contractor's applications.

55.11.3. Requirement Stage: All Contract Stages

55.12. Reference #2529: Identify and notify the Department of all errors and discrepancies found in the PBMS.

55.12.1. Contractor Approach: The Contractor shall put in place tools and procedures to validate the proper operation of the pharmacy enterprise. These tools and procedures shall include but are not limited to operational reporting, pharmacy help desk, technical help desk, and auditing. The Contractor shall identify all errors and discrepancies in the PBMS and notify the Department.

55.12.2. Deliverable: Error and Discrepancy Notification

55.12.3. Deliverable Stage: All Contract Stages

55.13. Reference #2530: Establish and lead cross contractor and Department operational status meetings, with other contractors such as the MMIS and BIDM contractors, when determined necessary by the Department.

55.13.1. Contractor Approach: Contractor shall establish, lead, and participate in operational status meetings with other contractors when appropriate or when determined necessary by the Department.

55.13.2. Requirement Stage: All Contract Stages

55.14. Reference #2531: Maintain in accordance with 45 CFR Part 74, accounting books, accounting records, documents, and other evidence pertaining to the administrative costs and expenses of this Contract to the extent and in such detail as shall properly reflect all revenues; all net costs, direct and apportioned; and other costs and expenses, of whatever nature, that relate to performance of contractual duties under the provisions of this Contract. The Contractor's accounting procedures and practices shall conform to generally accepted accounting principles, and the costs properly applicable to this Contract shall be readily ascertainable.

55.14.1. Contractor Approach: The Contractor shall establish a cost center within the Contractor’s accounting system in order to track revenue, direct expenses, and other allocated costs specific to the Contract.

55.14.2. The accounting system shall collect sufficient level of detail so as to support the costs/revenues that relate to performance of contractual duties.

55.14.3. The accounting system shall be maintained in compliance with generally accepted accounting principles (GAAP), and is subject to audit by independent CPA firms, internal audit, State and Federal Governments.

55.14.4. Contractor records shall be in compliance with 45 CFR Part 74.

55.14.5. Requirement Stage: All Contract Stages

55.15. Reference #2532: Assist Department staff and the Department's contractors with research, resolution, and response to client and provider issues related to the PBMS brought to the Department's attention.

55.15.1. Contractor Approach: The Contractor shall use the PBMS contact tracking and management system in the Pharmacy Support Center to record and track all inquiries and requests received from prescribers, pharmacy and members.

55.15.1.1. The Department staff shall be provided access to the Contractor's read-only application that allows authorized users to search form information pertaining to:

55.15.1.1.1. Member claims

55.15.1.1.2. Pharmacies

55.15.1.1.3. Drug coverage and information

55.15.1.1.4. Physician information

55.15.1.1.5. Prior authorization requests, including status

55.15.1.1.6. Call tracking notes

55.15.1.2. The Contractor shall provide assistance to the Department as requested by the Department.

55.15.2. Requirement Stage: All Contract Stages

55.16. Reference #2533: Manage, publish, update, index, and provide electronic public access via the MMIS website to all pharmacy related program communications, guides, forms, and files.

55.16.1. The items that the Contractor manages, publishes, indexes and provides electronic access to the public shall include, but not be limited to, the following:

55.16.1.1. Program newsletters.

55.16.1.2. Provider billing manuals, bulletins, announcements, and enrollment forms.

55.16.1.3. Transaction companion guides.

55.16.1.4. Procedure and diagnosis reference lists.

55.16.1.5. Frequently asked questions (FAQs).

55.16.2. Contractor Approach: The Contractor shall manage, publish, update, index, and provide electronic public access via the MMIS website to all pharmacy related program communications, guides, forms, and files including, but not limited to, the following:

55.16.2.1. Program newsletters

55.16.2.2. Provider billing manuals, bulletins, announcements, and enrollment forms

55.16.2.3. Transaction companion guides.

55.16.2.4. Procedure and diagnosis reference lists

55.16.2.5. Frequently asked questions (FAQs).

55.16.3. Requirement Stage: All Contract Stages

55.17. Reference #2534: Run all PDL activities, including all program activities, clinical review of PDL drug classes for clinical safety and efficacy. Make recommendations regarding preferred agents and potential PDL classes, contract negotiations for all supplemental rebates.

55.17.1. Contractor Approach: The Contractor shall run all PDL activities, such as activities described in this section.

55.17.2. The Contractor shall make available to the Department, at the Department's sole discretion, the option of participating in one of the Contractor's two CMS approved PDL pool programs (the National Medicaid Purchasing Initiative (NMPI) or the Optimal PDL $olution (TOP$).

55.17.2.1. The Contractor shall collaborate and assist the Department with all PDL relevant and necessary State Plan Amendment (SPA) submissions to CMS.

55.17.2.2. If the Department does not elect to join either NMPI or TOP$, the Contractor shall manage and administer the Contract negotiations for a Colorado state-specific supplemental drug rebate program.

55.17.2.3. The Contractor shall make recommendations as directed by the Department, but no more often than quarterly, for potential new drug classes to be added to the PDL.

55.17.2.4. The Contractor shall conduct cost analyses of therapeutic classes selected by the Department for inclusion on the PDL at prior to each P&T Committee meeting in accordance with Department rules. Analysis shall include detail for each drug in the class schedule for review,

55.17.2.5. The Contractor shall make available to the Department standard Therapeutic Class Reviews (TCRs) for all drug classes to be included on the PDL. TCRs shall be developed and maintained by the Contractor and are updated no less than annually. The Contractor shall solicit on a no less than annual basis, supplemental drug rebates from drug manufacturers.

55.17.2.6. The Contractor shall assist in facilitating all P&T Committee meetings, presenting of clinical and efficacy and financial data of PDL classes, in support of recommendations made to the Department for management of the PDL.

55.17.3. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

55.18. Reference #2535: Accept materials from third parties regarding PDL drug classes, and prepare meeting materials for the Pharmacy and Therapeutics (P&T) Committee.

55.18.1. Contractor Approach: The Contractor shall develop a Department approved process for obtaining and reviewing all PDL-related material submitted by third parties. The Contractor shall provide all PDL-related material to the P&T Committee.

55.18.1.1. The Contractor shall create P&T Committee meeting agendas, coordinate speakers, and provide meeting minutes to the Department for approval.

55.18.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

55.19. Reference #2536: Provide ongoing analysis and a clinical review of new name brand drugs for clinical safety and efficacy.

55.19.1. Contractor Approach: The Contractor shall support a clinical review of new name brand drugs for clinical safety and efficacy through interim drug monographs.

55.19.2. The Contractor shall provide support for each P&T Committee meeting by conducting a cost analysis for each class selected for review. The analysis shall include new brand name drugs, estimated market share by product, and any estimated cost savings.

55.19.3. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

55.20. Reference #2537: Provide ongoing analysis and a clinical review of new generic drugs for clinical safety and efficacy.

55.20.1. Contractor Approach: The Contractor shall provide support for each P&T Committee meeting by conducting a cost analysis for each class selected for review. The analysis shall include new generic drugs, estimated market share by product, and any estimated cost savings.

55.20.1.1. The Contractor shall support a clinical review of new generic drugs for clinical safety and efficacy through the yearly TCR updates or interim drug monographs.

55.20.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

55.21. Reference #2538: Provide ongoing analysis and a clinical review of existing drugs for new indications or changes to indications.

55.21.1. Contractor Approach: The Contractor shall provide support for each P&T Committee meeting by conducting a cost analysis for each class selected for review. The Contractor shall support a clinical review of existing drugs for new indications or changes to indications through the yearly TCR updates or interim drug monographs.

55.21.2. The Contractor shall provide clinical information regarding new indications or changes to indications, and recommendations on how to manage those changes, to the Department on an ongoing basis.

55.21.3. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

55.22. Reference #2539: Provide ongoing analysis and a clinical review of new product forms and strengths.

55.22.1. Contractor Approach: The Contractor shall provide support for each P&T Committee meeting by conducting a cost analysis for each class selected for review. The analysis shall include new product forms and strengths, estimated market share by product, and any estimated cost savings.

55.22.1.1. The Contractor shall support a clinical review of new product forms and strengths for clinical safety and efficacy through the yearly TCR updates or interim drug monographs.

55.22.1.2. The Contractor shall provide a weekly file of new GSNs and NDCs added to the PBMS and recommendations on the management of those new GSNs and NDCs.

55.22.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

55.23. Reference #2540: Facilitate P&T Committee meetings.

55.23.1. Meeting facilitation shall include, but is not limited to, all of the following:

55.23.1.1. Obtaining meeting location.

55.23.1.2. Arranging for parking.

55.23.1.3. Providing refreshments.

55.23.1.4. Creating agenda.

55.23.1.5. Coordinating speakers.

55.23.1.6. Providing meeting minutes.

55.23.2. Contractor Approach: The Contractor shall facilitate all Colorado P&T Committee meetings. The Contractor shall obtain a reasonable meeting location of sufficient capacity and capabilities that includes reasonable parking accommodations. The Contractor shall provide refreshments for P&T Committee members during the meeting.

55.23.2.1. The Contractor shall develop, for Department approval, P&T Committee meeting agendas and minutes, in accordance with Department policy. In addition, the Contractor shall coordinate all speakers registered to speak at the P&T Committee meeting.

55.23.3. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

55.24. Reference #2541: Based on supplemental rebate offers from manufacturers, clinical information, stakeholder input, and P&T recommendations, present PDL recommendations to the Department. The Department will use this information to make determinations on preferred and non-preferred drugs.

55.24.1. The Contractor shall complete this requirement at least once per calendar quarter. The Contractor shall meet with stakeholders, and shall be responsible for receiving and reporting on stakeholder recommendations. The Contractor shall send all escalations to the Department.

55.24.2. Contractor Approach: The Contractor shall support the Department's P&T process by providing a minimum of four cycles of analysis per year.

55.24.3. The Contractor's Clinical Pharmacist shall support the process by presentation of selected therapeutic class reviews and clinical recommendations. The Clinical Pharmacist shall meet with stakeholders and escalate issues to the Department as necessary.

55.24.4. Each cycle shall consist of a cost analysis that encompasses Colorado specific utilization, ingredient costs and dispensing fees, and all available Medicaid drug rebates.

55.24.5. This process shall include available feedback and recommendations available from relevant stakeholders in the process.

55.24.6. Requirement Stage: All Contract Stages

55.25. Reference #2542: Provide a mailroom and print center to support provider relationship management, claims/ encounters adjudication, and required client and provider communication functions.

55.25.1. Contractor Approach: The Contractor shall provide a mailroom supporting receipt of paper claims, provider communication distribution, incoming mail from providers and customers, and other documentation submitted to the Contractor regarding the PBMS, including paper claims processing and handling. The Contractor shall provide qualified employees and state-of-the-art systems that support paper claims processing to ensure that both HIPAA and Department-specific standards are upheld. The Contractor's

trained staff shall follow established procedures for claims receipt and control, security, and confidentiality.

55.25.2. Requirement Stage: PBMS Ongoing Operations and Enhancement Contract Stage

55.26. Reference #2543: Ensure that all project and Contract documents are made available on the electronic data repository and that all documents available on the repository are the most current and prior versions, as determined necessary by the Department, of the document available.

55.26.1. Contractor Approach: The Contractor shall maintain all project and Contract documents in the shared document repository. This system shall provide document versioning functionality to the Department staff enabling them to view the current and/or any prior version of a stored document. The shared document repository shall provide secure storage of these artifacts and shall be accessible by authorized Department users.

55.26.2. Requirement Stage: All Contract Stages

56. PHARMACY CLAIMS/ ENCOUNTER RELATED SERVICES

56.1. Reference #2544: THIS REQUIREMENT INTENTIONALLY DELETED

56.2. Reference #2545: Monitor claims/ encounter reports and claims/ encounter processing to ensure accuracy.

56.2.1. Contractor Approach: The Contractor shall monitor claims/encounter reports and claims/encounter processing to ensure accuracy.

56.2.2. The Contractor shall have established processes and procedures to monitor claims/encounter data through reporting and retrospective monitoring of the adjudication system. These processes shall be designed to ensure the integrity of the system as a whole and to minimize any undesired behavior.

56.2.3. Requirement Stage: All Contract Stages

56.3. Reference #2546: Document claims/ encounters billing processes, policies and procedures and make available online to users and providers.

56.3.1. Contractor Approach: The Contractor shall document claims and encounters billing processes, policies and procedure in the Pharmacy Billing Manual. The Contractor shall submit the manual to the Department prior to implementation for review and approval. Once approved, the Pharmacy Billing Manual shall be provided to the Department's MMIS contractor for placement on the Department Medicaid web site.

56.3.2. Requirement Stage: PBMS Implementation Contract Stage

56.4. Reference #2547: THIS REQUIREMENT INTENTIONALLY DELETED

56.5. Reference #2548: Apply voids and adjustments to the claims and encounters as identified by the Department's contractors or Department, within the claims/encounters processing cycle.

56.5.1. The Contractor shall apply voids and adjustments in the timeframe specified by the Department in order to be within the claims/encounters processing cycle.

56.5.2. Contractor Approach: The Contractor shall apply voids and adjustments identified by the Department within the claims/encounters processing cycle. The Contractor shall execute void and adjustment process within the claims/encounters processing cycle in the timeframe specified by the Department.

56.5.3. Requirement Stage: All Contract Stages

56.6. Reference #2549: Identify, analyze, and correct errors that have resulted in improper claims or encounters processing, such as if final edit dispositions are incorrect or there is an incorrect loaded rate, trace to the source, reprocess as needed, and report to the Department.

56.6.1. Contractor Approach: The Contractor shall identify, analyze, and correct errors that result in improper claims or encounters processing. If the final dispositions are incorrect, or there is an incorrect load, the Contractor shall trace to the source, correct, and reprocess as needed. The Contractor shall have established policies and procedures for retrospective internal monitoring and auditing of the claim adjudication system. These processes shall be designed to ensure the integrity of the adjudication system as a whole, and to minimize any undesired system behavior.

56.6.2. Requirement Stage: PBMS Implementation Contract Stage

56.7. Reference #2550: Provide the ability to price and process DME supplies in PBMS, such as any item with an NDC.

56.7.1. Contractor Approach: The Contractor shall process and price for durable medical equipment (DME) supplies as directed by the Department, such as any item with an active NDC in the drug file.

56.7.2. Requirement Stage: PBMS Implementation Contract Stage

56.8. Reference #2551: Provide the ability to pilot business rules to be applied to a designated group, such as Client or Provider, in a test environment. Provide the flexibility to add and change indicators and parameters easily and to allow for authorized user-defined adjudication rules.

56.8.1. Contractor Approach: The Contractor shall provide the ability to pilot business rules to be applied to a designated group (e.g., member, provider, or managed care organization) in a test environment. Operating under a single version of software, the PBMS shall be designed to be highly configurable to provide the flexibility to add and change indicators and parameters to achieve the desired adjudication outcome via user configuration.

56.8.2. Requirement Stage: All Contract Stages

57. PHARMACY PRIOR AUTHORIZATION SERVICES

57.1. Reference #2552: Coordinate and standardize processing and tracking of PAR data for purpose of utilization review.

57.1.1. Contractor Approach: The Contractor shall provide several methods and system solutions to coordinate and standardize processing and tracking of PAR data, utilizing Department approved clinical criteria for the purpose of utilization review. This shall include AutoPA, the manual PA process and POS which shall be configured to deliver consistent and repeatable PAR determinations.

57.1.2. Requirement Stage: All Contract Stages

57.2. Reference #2553: Provide the ability to identify, search, and report on PARs with potentially conflicting or duplicative data.

57.2.1. Contractor Approach: The Contractor shall use the PBMS contact tracking and management system to identify, search and report on PARs recorded in the database. The PBMS shall allow access to each prior authorization, inquiry, and override for questions and management reporting.

57.2.2. Requirement Stage: All Contract Stages

58. PHARMACY CALL CENTER SERVICES

58.1. Reference #2554: Maintain and staff a provider communications/relations function.

58.1.1. This provider communications/relations function shall include, but is not limited to, all of the following:

58.1.1.1. Providing and receiving communication from toll-free lines

58.1.1.2. Providing and email communications.

58.1.1.3. Providing webinar communication

58.1.1.4. Providing toll-free fax communication.

58.1.1.5. Providing an automated message informing the provider about hold and wait times.

58.1.1.6. Providing Colorado-specific staff during the Contractor's business hours defined in Reference #2111. Outside those hours the Contractor shall provide help desk resources, including an on call clinical pharmacist, but those resources may be shared with other entities and need not be Colorado-specific.

58.1.1.6.1. The Contractor shall make its Clinical Key Personnel available during business hours.

58.1.1.7. Maintaining a sufficient number of telephone lines, technology, and personnel so that all performance standards are met.

58.1.2. Contractor Approach: The Contractor shall utilize the PBMS call and documentation tracking system to receive and track inquiries via telephone, fax, and mail. The toll-free phone line shall be configured to receive and route calls. The Contractor shall also inform callers about hold and wait times. The Contractor shall provide a dedicated toll-free phone number and e-mail address.

58.1.2.1. The Contractor shall provide Colorado-specific staff during business hours to meet this requirement. After business hours, the Contractor shall provide help desk resources including an on-call clinical pharmacist.

58.1.3. Requirement Stage: All Contract Stages

58.2. Reference #2555: Provide the appropriate technical or operational support based on call issue, and provide the appropriate staff to answer the question(s).

58.2.1. Contractor Approach: The Contractor shall staff the Pharmacy Support Center and Clinical Support Center with fully trained licensed Clinical Pharmacists and Certified

Pharmacy Technicians (CPhTs) to handle inquiries/requests received about the Department's Medicaid pharmacy program from prescribers and pharmacies. The Contractor shall provide training to all Pharmacy Support Center and Clinical Support Center staff regarding Colorado-specific policies and procedures. The Contractor shall provide online help desk tools specific to the Department's program for reference in handling inquiries, such as system issues and PARs.

58.2.2. Requirement Stage: All Contract Stages

58.3. Reference #2556: Support an online provider complaint tracking, resolution, and reporting process that allows the Contractor to proactively identify trends. Contractor shall provide summary reporting to the Department on a routine basis.

58.3.1. Contractor Approach: The Contractor shall use the PBMS contact tracking and management system to record and track all inquiries received from prescribers and pharmacies. The PBMS shall be a flexible tool that provides the ability to record a variety of call data to include call category, call type and response. This capability shall allow for reporting of trends and analysis. The Contractor shall provide a summary report to the Department and based on the Department's specific needs on a monthly basis.

58.3.2. Requirement Stage: All Contract Stages

58.4. Reference #2557: THIS REQUIREMENT INTENTIONALLY DELETED

58.5. Reference #2558: Provide and maintain an Interactive Voice Response (IVR) function that provides callers with straightforward menu options to reach the appropriate prerecorded information or a live operator.

58.5.1. Contractor Approach: The Contractor shall provide an automated call distribution system that permits efficient management of calls and staff assignments. The Contractor shall configure the system with customized routing and/or messages specified and approved by the Department. The Contractor's IVR solution shall be used to support appropriate call routing and messaging, and to help decrease the providers' administrative burden.

58.5.2. Requirement Stage: All Contract Stages

58.6. Reference #2559: Provide a dedicated inbound email address for providers to use as part of the Customer Service Center.

58.6.1. Contractor Approach: The Contractor shall provide a dedicated inbound e-mail address for providers to submit questions. The Contractor shall monitor this e-mail box and resolve and respond to the request.

58.6.2. Requirement Stage: All Contract Stages

58.7. Reference #2560: Provide the Department with monthly reports on all inquiries, the nature of the inquiries, and the timeliness of responses to inquiries for the call center and help desk activity.

58.7.1. Contractor Approach: The Contractor shall provide call center-related reports and monthly trend analyses regarding telephone, fax, and prior authorization activity by call center staff per the Department's specific requirements.

58.7.2. Requirement Stage: All Contract Stages

58.8. Reference #2561: Provide a centralized call center and help desk database or reporting capability that creates, edits, sorts, and filters tickets or electronic records of calls made to the call center and help desk categories that can be accessed and utilized by the Department for provider and client tracking and management.

58.8.1. Contractor Approach: The Contractor shall record and track all inquiries received from prescribers and pharmacies in the PBMS. The Contractor shall utilize the Contractor's call management system to provide real-time reporting on Call Center activity. Contractor shall track metrics regularly and offer reporting services that show performance based on service level agreements. Capabilities shall include editing, sorting and filtering.

58.8.2. Requirement Stage: PBMS Ongoing Operations and Enhancements Contract Stage

58.9. Reference #2562: The Contractor shall staff a Call Center/ Help Desk from 8:00 am to 5:00 pm Mountain Time, Monday - Friday.

58.9.1. Contractor Approach: The Contractor shall provide the Department a dedicated team of Pharmacists, CPhTs and Senior CPhTs who shall be available from 8:00 am to 5:00 pm Mountain time, Monday through Friday.

58.9.2. Requirement Stage: All Contract Stages

58.10. Reference #2563: THIS REQUIREMENT INTENTIONALLY DELETED

58.11. Reference #2564: THIS REQUIREMENT INTENTIONALLY DELETED

58.12. Reference #2565: Provide call-center, help desk, web knowledge base forum and other support to users, including PBMS and Provider Enrollment support.

58.12.1. Contractor Approach: The Contractor shall provide call-center, help desk, web knowledge base forum and other support for the Department's prescribers and pharmacies to include prior authorization, technical assistance with claims submission, billing issues, drug coverage, eligibility, policy and procedural information, COB payer information, early refill and other ProDUR and clinical edit override authorization, and member support. Provider enrollment support shall include receiving the call and determining if the issue requires enrollment related resolution by the MMIS and, if so, directing the provider to the appropriate MMIS contact.

58.12.2. Requirement Stage: All Contract Stages

59. PHARMACY HELP DESK SERVICES

59.1. Reference #2566: Maintain a Help Desk for all System users.

59.1.1. The Contractor shall provide Colorado-specific staff during the Contractor's business hours defined in Reference #2111. Outside those hours the Contractor shall provide help desk resources for this requirement but those resources may be shared with other entities and need not be Colorado-specific.

59.1.2. Contractor Approach: The Contractor shall provide a pharmacy help desk for external PBMS users and an IT help desk for Department users to contact for IT-related issues,

such as system access issues. The IT help desk shall contain Contract-specific staff during business hours.

59.1.3. Requirement Stage: All Contract Stages

60. DRUG REBATE SUPPORT SERVICES

60.1. Reference #2567: Track payments to appropriate calendar quarter.

60.1.1. Contractor Approach: The Contractor shall submit invoices and enter payments to the appropriate invoice, at the NDC 11 level. Payments shall be tracked at a quarterly level.

60.1.2. Requirement Stage: All Contract Stages

60.2. Reference #2568: Track payments by labeler.

60.2.1. Contractor Approach: The Contractor shall submit invoices and enter payments to the appropriate invoice, at the NDC 11 level. Payments shall be tracked at a labeler level.

60.2.2. Requirement Stage: All Contract Stages

60.3. Reference #2569: Record all receipts of rebate payments, distinguish between federal and supplemental rebates and distinguish between rebates for claims and rebates for encounters.

60.3.1. Contractor Approach: The Contractor shall utilize its rebate administration tool in the administration (process, invoice and collection) of both the Colorado Federal and Supplemental rebate programs.

60.3.1.1. This modular, rules-based system shall allow for flexibility in establishing independent program needs to accommodate differences in the Federal (OBRA, MCO) and Supplemental contracts, as well as support of Diabetic Supply or Commercial programs.

60.3.1.2. The Contractor shall create separate quarterly invoices for Supplemental versus Federal rebates for each labeler; the Contractor shall record and track receipts to distinguish Supplemental and Federal rebates from each other.

60.3.2. Requirement Stage: All Contract Stages

60.4. Reference #2570: Represent Department in dispute resolution meeting with labelers, including, but not limited to out-of-state conferences designed for that purpose, as requested by the Department.

60.4.1. Contractor Approach: The Contractor shall engage in continuous dispute resolution. In addition, the Contractor shall represent the Department at dispute resolution meetings and any out-of-state conferences, at the Department's request.

60.4.2. Requirement Stage: All Contract Stages

60.5. Reference #2571: Receive supplemental rebate agreements from manufacturers. Ability to receive the Guaranteed Net Unit Price (GNUP) into the System.

60.5.1. Contractor Approach: Manufacturers shall be solicited for GNUP offers and instructed to submit their offers in a specified format to a pre-determined FTP site. Once received, each offer shall be validated and uploaded into the Contractor's proprietary offer

system. Following validity analysis of the offers, Supplemental Rebate Agreements shall be generated from the offer system and sent to the manufacturer for signature prior to each P&T Committee Meeting to ensure the manufacturer's agreement with all applicable terms and conditions. Once signed by the manufacturer, the Supplemental Rebate Agreements shall be held at the Contractor's office until results of the P&T Committee meeting are known. Applicable supplemental rebate agreements shall be forwarded to the Department for signature. Any supplemental rebate agreement that is executed shall be entered into the rebate administration system for supplemental rebate invoicing purposes.

60.5.2. Requirement Stage: All Contract Stages

60.6. Reference #2572: Contractor shall have reporting capabilities that coincide with the Department's needs for CMS64.

60.6.1. Contractor Approach: The Contractor shall comply with all CMS reporting requirements during the Contract, including producing data for the CMS 64.9R quarterly report.

60.6.1.1. The Contractor shall provide all required drug rebate data to the MMIS including all drug rebate related data from its system needed to produce the CMS 64.

60.6.2. Requirement Stage: All Contract Stages

61. INVOICING

61.1. Reference #2573: The Contractor shall invoice the Department on a monthly basis, by the fifteenth (15th) Business Day of the month following the month for which the invoice covers. The Contractor shall not submit any invoice for a month prior to the last day of the month the invoice covers.

61.1.1. Contractor Approach: The Contractor shall deliver a monthly invoice to the Department by the fifteenth Business Day of the month following the month for which the work occurs. At the close of the month, the Contractor shall utilize an invoicing checklist to ensure all invoices are prepared completely, accurately, and timely (not prior to the last day of the month in the invoicing period, and not after the 15th Business Day in the following month) and delivered to the Department for payment.

61.1.2. Requirement Stage: All Contract Stages

61.2. Reference #2574: The monthly operating payment invoice shall contain all information as directed by the Department,

61.2.1. This information shall include all of the following for the month for which the invoice covers:

61.2.1.1. All necessary information for the Department to determine the accuracy of the invoice and properly pay the invoice to the Contractor.

61.2.1.2. The Contractor shall provide all invoices in a format as approved by the Department

61.2.2. Contractor Approach: The Contractor shall invoice for Ongoing Operations and Enhancements Contract Stage for the following elements:

61.2.2.1. Fixed Monthly Ongoing Operations and Enhancements Contract Stage Payments; Provide pricing, independent of the PBMS Implementation Contract Stage, that is specifically related to the provision of PBMS Ongoing Operations and Enhancements Contract Stage

61.2.2.2. Quality Maintenance Payments; The Contractor shall provide a fixed price for the complete Contract Stage over the State Fiscal Year (SFY) (ending June 30) that includes fixed monthly payments over the estimated period of the Contract Stage and the Quality Maintenance Payments dollar amount as described in Exhibit E, Compensation and Quality Maintenance Payments Section 2.

61.2.2.3. The Contractor shall provide all necessary supporting reports and other documentation required to support customer billing. System generated reports shall be provided to support member counts, claims volume, prior authorizations, billable hours or any other metric-based customer billing.

61.2.2.4. The Contractor shall maintain several internal systems providing source documentation used to support invoicing. These systems include the claims adjudication system (FirstRx), call tracking and monitoring systems (FirstTrax), and time reporting applications (Remedy Time Reporting, WebSPR).

61.2.3. Requirement Stage: All Contract Stages

Contract Routing Number 20160000000000002089

EXHIBIT D, PROJECT PHASE DOCUMENT

These Project Phases apply to the PBMS Implementation Contract Stage. The items listed in each row may occur concurrently throughout the applicable Project Phase, or may cross into other Project Phases. The bulleted items indicate that there are multiple items in that category, and are not aligned in any specific order across the row.

PBMS Development Project Phases:

The following tables apply to the PBMS system development Project Phases. As opposed to the PBMS Operations Project Phases at the end, these tables reflect the responsibilities of the Contractor and the Department in developing, Configuring, testing, and CMS certification of the PBMS component of the MMIS enterprise or the entire MMIS enterprise, which includes the PBMS.

The Initiation and Planning Phase: includes the Department's and Contractor's initial project planning and set up activities. This includes activities to promote project planning, bi-directional knowledge transfer, improving the Contractor's understanding of the Colorado Medical Assistance program via familiarization activities, communication, and team-building activities to develop a collaborative working relationship between the Department and Contractor. The Contractor shall work with the Department to establish key project planning documents and Deliverables, including the Work Breakdown Schedule, Risk Management Plan, Communication Management Plan, Change Management Plan, and Resource Management Plan as detailed in Exhibit C, Requirements.
Entrance Criteria: • The Effective date of the Contract • State and federal authorities have approved the Contract.
Exit Criteria: • Completion of the Project Kick-Off Meeting. • Department approval of all Initiation and Planning Deliverables.

#	Contractor Responsibilities	Department Responsibilities
1.	Conduct a Project Kick-Off Meeting with key stakeholders and the Department project team that meets, at minimum, the following objectives: • Introduce project team and stakeholders. Review the project mission and guiding principles. • Determine the format and protocol for ongoing project status meetings. • Review the project Deliverable schedule and review process. • Identify project risks and mitigation process. • Communicate the issue identification and risk process.	• Participate in the Project Kick-Off Meeting. • Provide the necessary education and documentation to appropriate Contractor staff to ensure Contractor is adequately trained on applicable Department policies and procedures.
2.	Establish a Project Management Plan.	Collaborate with the Contractor in order to review and approve the Project Management Plan.
3.	Establish a Project Control and Issue Reporting System.	Collaborate with the Contractor in order to review and approve the Project Control and Issue Reporting System.
4.	Collaborate with the Department to finalize a Detailed Work Breakdown Structure and Schedule.	Collaborate with the Contractor in order to review and approve a baseline of the Detailed Work Breakdown Schedule.
5.	Establish an Electronic Document Repository.	Collaborate with the Contractor to obtain access to the Electronic Document Repository.
6.	Collaborate with the Department to finalize and document the entrance and exit criteria for each Project Phase, as well as the Department's process for validating that entrance and exit criteria were met.	Work with the Contractor to establish and document entrance and exit criteria for each Project Phase.

#	Contractor Responsibilities	Department Responsibilities
7.	Develop a Risk Management Plan.	Collaborate with the Contractor in order to review and approve the Risk Management Plan.
8.	Develop a QA Control/Quality Management Plan.	Collaborate with the Contractor in order to review and approve the QA Control/Quality Management Plan.
9.	Develop and submit the Resource Management Plan.	Collaborate with the Contractor in order to review and approve the Resource Management Plan.
10.	Develop and submit the Change Management Plan.	Collaborate with the Contractor in order to review and approve the Change Management Plan.
11.	Not Used	Not Used
12.	Develop and submit the Business Continuity and Disaster Recovery Plan.	Collaborate with the Contractor in order to review and approve the Business Continuity and Disaster Recovery Plan.
13.	Develop and submit the Communication Management Plan that includes reporting templates, and Deliverable review and acceptance procedures.	Collaborate with the Contractor in order to review and approve the Communication Management Plan.
14.	Develop and submit a Gate Review Crosswalk.	Collaborate with the Contractor and the Colorado Governor's Office of Information Technology (OIT) in order to review and approve the Gate Review Crosswalk.
15.	Review progress and compliance with Initiation and Planning Phase entrance and exit criteria as agreed upon by the Contractor and Department.	Review progress and compliance with Initiation and Planning Phase entrance and exit criteria.

#	Contractor Responsibilities	Department Responsibilities
16.	Develop and submit all Initiation and Planning Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Initiation and Planning Phase Deliverables and provide the Contractor with necessary access to documentation to complete the Initiation and Planning Phase Deliverables.

Discovery and Requirements Validation/Requirements Elicitation Phase: In this Project Phase, the Contractor shall work with Department personnel to validate and further define the System architecture and requirements, and reconcile them against Contractor-proposed solutions. The primary Deliverables produced during this Project Phase are the Requirements Specification Document (RSD) and a RTM, as detailed in Exhibit C, Requirements, to ensure requirements are adequately tracked and managed.
Entrance Criteria: • The Department delivers the future-state business processes, as referenced in the State Self-Assessment (SSA), the Department's Use Case Report (referenced in the SSA), and the Recommendations Report resulting from the completion of the CORE MMIS Business Process Re-Engineering Stage to the Contractor.
Exit Criteria: • Completion of all agreed upon Requirement Review and Validation Sessions, which includes Department acceptance of all session results. • Department acceptance of the RSD and RTM.

#	Contractor Responsibilities	Department Responsibilities
17.	Utilize Requirements Review and Validation Sessions to gain an understanding of user sophistication, which should be applied to the development of training programs and user documentation.	• Provide appropriate staff to attend Requirement Review and Validation Sessions. • Work with the Contractor to establish schedule and location for Requirement Review and Validation Sessions.
18.	Develop and submit a Requirements Definition and Validation Plan.	Collaborate with the Contractor in order to review and approve the Requirements Definition and Validation Plan.

#	Contractor Responsibilities	Department Responsibilities
19.	Prepare and submit the Requirement Review and Validation Session meeting notes. Include decisions, justification for changes, outstanding issues requiring follow-up, and impacts to future sessions and session participants.	• Review and approve the Requirement Review and Validation Session meeting notes. • Forward the meeting notes to the appropriate staff.
20.	Use project control tools to formally track session results and allow the Contractor/Department to manage the requirements decisions by module or functional area. The tools should also provide the ability to manage requirements not yet completed, as well as decisions from completed requirement review and validation sessions.	• Review and respond to all requirement change documents, using the agreed-upon project Change Management Process. • Track policy-related changes and training impacts identified during the Requirement Review and Validation Sessions.
21.	Develop and submit to the Department a draft Requirements Specifications Document (RSD) for Contractor-proposed System components, modules and functional areas.	• Collaborate with the Contractor in order to review and approve the Detailed Requirements Specification Template. • Collaborate with the Contractor in order to review and provide feedback on the draft RSD.
22.	Compile the final RSD.	Collaborate with the Contractor in order to review and approve the final RSD.
23.	Develop and maintain a Business Rules Traceability Matrix.	Collaborate with the Contractor in order to review and approve the Business RTM.
24.	Develop and maintain a RTM.	Collaborate with the Contractor in order to review and approve the RTM.

#	Contractor Responsibilities	Department Responsibilities
25.	Review proposed business rules with the Department and conduct a gap analysis to compare the proposed business rules against the Department's existing business rules to identify additional business rules required for the System.	
26.	Not Used	Not Used
27.	Review progress and compliance with the Discovery and Requirements Validation/Requirements Elicitation Phase entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance with Discovery and Requirements Validation/Requirements Elicitation Phase entrance and exit criteria.
28.	Develop and submit the Discovery and Requirements Validation/Requirements Elicitation Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Discovery and Requirements Validation/Requirements Elicitation Phase Deliverables and provide the Contractor with necessary access to documentation to complete the Discovery and Requirements Validation/Requirements Elicitation Phase Deliverables.

Design and Definition Phase: This Project Phase includes the development (for functionality not proposed as a COTS product) and validation of design specifications or product documentation for System screens, reports, data, interfaces, and business rules that conform to requirements that were validated during the Discovery and Requirements Validation/Requirements Elicitation Phase.
Entrance Criteria: • Department acceptance of business process improvements of the business process maps, which result from the Requirements Specification Document (RSD), the Business RTM, and the outputs of the Business Process Re-Engineering Stage - the Recommendations Report and the Action Plan. • Department acceptance of the RSD and RTM.
Exit Criteria: • Completion of all agreed upon Detailed System Design Sessions, which includes Department acceptance of all session results. • Department acceptance of the Design Specification Document (DSD) for non-COTS components and RTM.

#	Contractor Responsibilities	Department Responsibilities
29.	Develop and submit a Detailed System Design Plan for non-COTS components.	• Provide the Contractor with the necessary information and clarification regarding existing interfaces and System processes, as well as Department business rules, policies, regulations, and procedures. • Collaborate with the Contractor in order to review and approve the Detailed System Design Plan.
30.	Develop and submit a Detailed System Design Session schedule for review by the Department.	Work with the Contractor to establish schedule and location for Detailed System Design Sessions.
31.	Develop and distribute session agendas prior to each session.	Review and approve the Detailed System Design Session Agendas prior to each session.

#	Contractor Responsibilities	Department Responsibilities
32.	Conduct Detailed System Design Sessions to validate requirements with authorized users and other stakeholders.	Provide appropriate staff to attend Detailed System Design Sessions.
33.	Develop and submit a Physical System Security Plan.	Review and approve the Physical System Security Plan.
34.	Develop and submit an Environment Architecture and Implementation Plan.	Review and approve the Environment Architecture and Implementation Plan.
35.	Perform prototyping when appropriate to enable Department staff to review and accept windows, screens, reports or other layouts designs. Including an Online Application Template and Reporting Templates	Review and approve prototypes and templates.
36.	Demonstrate System component/module functionality through models and prototypes as appropriate.	• Provide staff to attend System component/module walkthroughs as necessary. • Review and approve application design mock-ups. • Review and approve the Environment Architecture and Implementation Plan. • Review and approve any System-generate reports. • Review and approve Templates of any Standard System Reports.
37.	Provide qualified data modelers and conduct any modeling sessions needed for data model modification.	
38.	Prepare and submit the Detailed System Design Session meeting notes.	Review and approve the Detailed System Design Session meeting notes.

#	Contractor Responsibilities	Department Responsibilities
39.	Use project control tools to formally track session results and allow the Contractor/Department to manage the design decisions by module or functional area. The tool should also provide visibility to outstanding decisions, as well as decisions resulting from completed Detailed System Design Sessions.	• Track policy-related changes and training impacts identified during the detailed design and definition sessions. • Review and respond to all Detailed System Design requirements change documents, using the agreed-upon project Change Management Process.
40.	Submit a draft Design Specification Document (DSD) that incorporates comments submitted by the Department.	Collaborate with the Contractor in order to review and approve the draft DSD.
41.	Conduct technical reviews of the DSD Deliverable with the Department to verify the design and resolve design issues or questions.	
42.	Develop a final DSD based on the facilitated design sessions.	• Collaborate with the Contractor in order to review and approve the final DSD. • Collaborate with the Contractor in order to review and approve the Systems Documentation Template.
43.	Update and maintain the RTM with results from Detailed System Design Sessions.	Review and approve the updated RTM.
44.	Review progress and compliance with Design and Definition Phase entrance and exit criteria as agreed upon by the Contractor and Department.	Review progress and compliance with Design and Definition Phase entrance and exit criteria.
45.	Develop and submit the Design and Definition Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Design and Definition Phase Deliverables and provide the Contractor with necessary access to documentation to complete the Design and Definition Phase Deliverables.

Development Phase: The Contractor shall develop the pieces of the System in this Project Phase if they are not part of the COTS product being Configured. The Contractor shall utilize development tools and established methodologies for maintaining control of the process and ensuring that the System components and architecture conforms to the requirements as documented in the prior Project Phases. The Development Phase shall include unit testing to verify that each basic component of the System is developed correctly in accordance with the design specifications.
Entrance Criteria: • Completion of all agreed upon Detailed System Design Sessions, which includes Department acceptance of all session results. • Department acceptance of the Design Specification Document and updated RTM.
Exit Criteria: • Facilitation of functionality walkthroughs with the Department. • Department approval of all Unit Test Checklists. • Department approval of each System module/functional component.

#	Contractor Responsibilities	Department Responsibilities
46.	Ensure that the Change Management Plan contains a Configuration Management component to identify the tools to be used to manage changes to the System components and modules.	Review, provide feedback, and approve the Configuration Management component of the Change Management Plan.
47.	Submit Change Management artifacts (Change Requests) as necessary.	Review, provide feedback, and approve Change Requests as necessary.
48.	Develop the System per approved design specifications.	
49.	Develop and submit to the Department a Unit Test Checklist Template and Unit Test Plan.	• Review and approve the Unit Test Checklist Template. • Review and approve the Unit Test Plan.

#	Contractor Responsibilities	Department Responsibilities
50.	Conduct unit testing and submit results via Unit Test Checklists.	Review and approve the Unit Test Results.
51.	Provide weekly updates and performance metrics on unit testing and development progress to the Department as part of the weekly status reports defined in Exhibit C, Requirements.	• Review and approve the Technical and Functional Documentation. • Participate in weekly updates and review performance metrics on unit testing and development progress.
52.	Develop System and user documentation as required.	Review and approve Contractor documentation that all System functions according to Department specifications.
53.	Conduct development walkthroughs for non-COTS components as appropriate to demonstrate to the Department that all System functions have been completely and accurately developed and unit-tested and record problems using the Project Control and Issue Reporting System described above.	Attend code walkthroughs as necessary.
54.	Review progress and compliance with Development Phase entrance and exit criteria as agreed upon by the Contractor and Department.	Review progress and compliance with Development Phase entrance and exit criteria.
55.	Develop and submit the Development Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review the Development Phase Deliverables and provide the Contractor with access to documentation necessary to complete the Development Phase Deliverables.

Data Conversion Phase: The Contractor shall work with Department staff to convert data contained in Legacy System to the PBMS according to the agreed upon Data Conversion Plan described in Exhibit C, Requirements. The Contractor shall plan,

test, and manage the data conversion process. The Department will provide the Contractor with the appropriate access to external systems and Department staff necessary to fully execute the Data Conversion Plan.
Entrance Criteria: • The entrance criterion for the Data Conversion activities is to define and document the source/legacy systems and obtain Department approval.
Exit Criteria: • The exit criterion for the Data Conversion activities is the Department's acceptance of migrated data from source or Legacy Systems into the PBMS.

#	Contractor Responsibilities	Department Responsibilities
56.	Develop and submit a phased Data Conversion Plan that provides detailed requirements.	• Provide and coordinate the appropriate Department source/legacy system resources during the Data Conversion Phase. • Verify that the System and associated documentation, tools are received from source or Legacy System and transferred to the Contractor, as available. • Act as liaison between the current Department systems resources and Contractor during the Data Conversion Phase. • Provide listing of system job cycles in use in source/legacy systems, as available, at time of transfer and installation. • Review and approve the Data Conversion Plan.

#	Contractor Responsibilities	Department Responsibilities
57.	Ensure that third party data acquisition requirements, including any additional costs and related agreements, are accounted for and included within the Data Conversion Plan. The Department will not be liable for any delays or fees incurred in data acquisition tasks.	
58.	Complete the discovery and evaluation tasks.	
59.	Acquire the hardware and software needed for a successful data conversion.	
60.	Implement a fully functioning data migration environment to be used by both the Contractor and Department for current and ongoing migration needs.	Collaborate with the Contractor in order to review and approve the migration environment.
61.	Coordinate with the Department to assign qualified access rights and resolve problems encountered during the conversion.	Coordinate with the Contractor to assign qualified access rights and resolve problems encountered in the conversion.
62.	Ensure that the hardware, software, protocols, processes, and communications are appropriately established, documented, and repeatable by authorized Department staff.	
63.	Revise System and user documentation as required.	Review and approve Contractor documentation that all System required data is transferred and functions according to Colorado specifications.
64.	Implement code modifications to the System as necessary for accurate operation of the System, including any future data conversion needs.	

#	Contractor Responsibilities	Department Responsibilities
65.	Perform a System test to compare all transferred programs, files, utilities, etc., to determine that the migration was successful.	Review and approve the Data Conversion Test Results.
66.	Assist the Department with issue identification and resolve program errors and rerun unit tests as necessary.	Identify issue(s) and assist the Contractor in resolving program errors.
67.	Incorporate data conversion progress in written status reports throughout the Data Conversion Phase.	Review and approve System modifications or miscellaneous documentation made by the Contractor during the Data Conversion Phase.
68.	Work with other System Contractor(s) and the Department to establish and ensure appropriate System and business interfaces as deemed necessary by the Department and/or federal requirements to successfully meet the responsibilities identified for this Project Phase.	Assist the Contractor in identifying the appropriate System and business interfaces.
69.	Review progress and compliance with Data Conversion Phase entrance and exit criteria as agreed upon by the Contractor and Department.	Review progress and compliance with Data Conversion Phase entrance and exit criteria.
70.	Develop and submit all Data Conversion Phase Deliverables as detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Data Conversion Phase Deliverables and provide the Contractor with necessary access to documentation to complete the Data Conversion Phase Deliverables.

Testing Phase: The Contractor shall test the replacement of the System software and hardware for compliance with defined requirements. The Contractor shall ensure that all testing activities, as described in this exhibit, are executed and that each System component meets or exceeds all of the functional, technical, security, and performance requirements prior to implementing the PBMS. The Department requires formal UAT. Department testers will be responsible for conducting UAT and signing off on the System functionality prior to it being released into production. Parallel testing activities in this Project Phase specifically relate to System functionality, and will be independent of parallel testing activities that will occur within the PBMS Operations scope. The Contractor may also propose additional tests that may maximize performance and/or operational readiness. All testing will be deemed complete only when written Department acceptance is obtained.
Entrance Criteria: • The entrance criterion for the Testing activities is the identification, documentation, and Department approval of defect/issue severity definitions.
Exit Criteria: • The exit criterion for the Testing activities is completion of all Test Cases for each testing sub-phase, documented and approved by the Department.

#	Contractor Responsibilities	Department Responsibilities
71.	Develop a System Test Plan that describes its approach and commitment to all testing sub-phases required for a System of this magnitude.	• Collaborate with the Contractor to review and approve the System Test Plan. • Collaborate with the Contractor to review and approve the System Test Template.
72.	Develop a Parallel Test Plan for testing the Contractor's implementation against the Legacy System.	Collaborate with the Contractor to review and approve the Parallel Test Plan.

#	Contractor Responsibilities	Department Responsibilities
73.	Provide all tools used to facilitate the testing process, including performance testing. The Department will not procure testing tools for this project and any testing tools proposed shall be provided by the Contractor and licensed by the Contractor for use by its staff and the applicable Department staff for the project at the testing site.	• Coordinate with Contractor the successful set-up of all required environments. • Act as liaison between the current Department System resources and Contractor during the Testing Phase. • Arrange for the transfer of any relevant Department software and files to the new Contractor, as available and as needed.
74.	Provide any required training on the proposed testing tools to all Department staff that will be required to use these tools.	• Identify and provide the appropriate staff to participate in any required training. • Collaborate with the Contractor to schedule training.
75.	Revise, implement, and document detailed Test Cases for each sub-phase of testing identified above.	• Approve all Test Cases prior to testing and reserve the right to request that additional Test Cases be developed and tested. • Provide necessary Department resources to participate in UAT.
76.	Provide the Department with testing progress, as part of the weekly status reports including, at minimum: • The number of issues identified. • Type. • Severity. • Mitigation strategy. • Projected resolution date.	• Review and approve Contractor documentation that all System required data is transferred and functions according to Colorado specifications. • Act as mediator to resolve any System installation problems. • Review and approve System modifications or miscellaneous documentation made by the Contractor during the Testing Phase.
77.	Finalize the severity definitions and determination process for with the Department. The Department shall maintain final authority on all severity assignments.	Approve the severity definitions and determination process for defects.

#	Contractor Responsibilities	Department Responsibilities
78.	Ensure all testing, issue resolution, and code promotion activities maintain zero impact to Department day-to-day operations.	Inform the Contractor of any day-to-day operations issues.
79.	Work with other System Contractor(s) and the Department to establish and ensure appropriate System and business interfaces as deemed necessary by the Department to successfully meet the responsibilities identified for this Project Phase.	Coordinate the appropriate Department and System resources during the installation of any telecommunications links to the Department's network, if needed.
80.	Submit all Test Results for each test sub-phase to the Department.	• Review and approve Performance/Stress Testing Results. • Review and approve Final System Test Results. • Review and approve Penetration Test Results. • Review and approve Parallel Test Results.
81.	Perform regression testing for all defects identified as directed by the Department.	• Assist the Contractor with regression testing and identify defects. • Review Regression Testing Results.
82.	Review progress and compliance with Testing Phase entrance and exit criteria as agreed upon by the Contractor and Department.	Review progress and compliance with Testing Phase entrance and exit criteria.
83.	Develop and submit all Testing Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Testing Phase Deliverables and provide the Contractor with necessary access to documentation to complete the Testing Phase Deliverables.
83a.	Design and document initial detailed Test Cases for UAT.	Review and approve all Test Cases prior to testing and reserve the right to request that additional Test Cases be developed and tested.

Organizational Readiness and Training Phase: The Contractor shall train Department staff and any affected Department contractors in System functionality and business processes required for successful implementation. Authorized users shall be proficient in using the System in order to ensure effective and efficient business operations.
Entrance Criteria: • Completion of UAT. • Establishment of the training environment.
Exit Criteria: • The exit criterion for the Training activities is completion of all scheduled Department training sessions.

#	Contractor Responsibilities	Department Responsibilities
84.	Within the Resource Management Plan submitted for Department approval, include a Training Plan that meets the requirements in Exhibit C, Requirements.	Provide feedback on the proposed Training Plan section of the Resource Management Plan, approach, and training materials prior to training sessions occurring or materials being released.
85.	Maintain and update the training environment with training data to use during training.	Review and approve the training environment and training content.
86.	Provide regular refresher training sessions for authorized System users to disseminate updated or new functionality or business processes related to the System throughout the Contract term, extending as agreed upon.	Provide any necessary feedback on training sessions.
87.	Review progress and compliance with Organizational Readiness and Training Phase entrance and exit criteria as agreed upon by the Contractor and Department.	Review progress and compliance with Organizational Readiness and Training Phase entrance and exit criteria.

#	Contractor Responsibilities	Department Responsibilities
88.	Develop and submit all Organizational Readiness and Training Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Organizational Readiness and Training Phase Deliverables and provide the Contractor with necessary access to documentation to complete the Organizational Readiness and Training Deliverables.

Implementation and Rollout Phase: The Contractor shall deploy the System in compliance with the agreed upon implementation approach. The Contractor shall manage the end-to-end implementation and establish a clear plan, project guidelines, implementation approach, and governance structure. The Contractor shall also help develop and manage the rollout plan, which shall include detailed planning and roadmaps for all releases. This includes the development of release management processes for Technology Stacks, databases, and infrastructure. This Project Phase will be considered complete when the Department accepts the System as operational based on predefined acceptance criteria.
Entrance Criteria: • The entrance criterion for Implementation and Rollout Phase activities is the completion of all scheduled Department training sessions.
Exit Criteria: • Completion and Department acceptance of the Operational Readiness Walkthrough. • Department acceptance of the System as operational.

#	Contractor Responsibilities	Department Responsibilities
89.	Develop an Implementation Strategy in conjunction with the Department System acceptance procedures.	• Work with the Contractor to determine the Implementation Strategy and schedule. • Collaborate with the Contractor in order to review and approve an Implementation Strategy.
90.	Conduct an Operational Readiness Walkthrough with the Department prior to the initial PBMS Implementation and Rollout Phase.	Participate in Operational Readiness Walkthroughs and provide formal acceptance of each Walkthrough once approved by the Department.
91.	Develop a "Go-Live" Support Plan that documents the onsite and offsite user support provided by the Contractor and Department during the initial System implementation.	Collaborate with the Contractor to review and approve the "Go-Live" Support Plan.

#	Contractor Responsibilities	Department Responsibilities
92.	Develop an Implementation and Rollout Plan that details planning and roadmaps for managing all System releases (if applicable).	Collaborate with the Contractor in order to review and approve the Implementation and Rollout Plan.
93.	Develop a Post-Implementation Operational Monitoring Plan, including methods and schedules for the Department and the Contractor to conduct post-implementation monitoring of System operations related to performance expectations as described in the Exhibit C, Requirements.	Collaborate with the Contractor in order to review and approve the Post-Implementation Operational Monitoring Plan.
94.	Monitor the initial operation of the System to ensure that there are no immediate or ongoing adverse effects on the Department programs according to the performance expectations as described in the Exhibit C, Requirements.	Identify any issues for the Contractor.
95.	Update System documentation and operating procedures with lessons learned from the Implementation and Rollout Phase.	Review and approve the updated System and Operational Documentation.
96.	Report on post-implementation issues and success for the System.	Review report and provide any necessary feedback on post-implementation issues.
97.	Identify and report any implementation issues to Department using the criteria.	Review report and provide any necessary feedback on any implementation issues.
98.	Obtain formal Department approval for the implementation of the System.	Provide formal acceptance of the implementation of the System once approved by the Department.
99.	Prepare a Post-Implementation Evaluation Report.	Collaborate with the Contractor in order to review and approve the Post-Implementation Evaluation Report.

#	Contractor Responsibilities	Department Responsibilities
100.	Review progress and compliance with Implementation and Rollout Phase entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance with Implementation and Rollout Phase entrance and exit criteria.
101.	Develop and submit all Implementation and Rollout Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Implementation and Rollout Phase Deliverables and provide the Contractor with necessary access to documentation to complete Implementation and Rollout Phase Deliverables.
102.	Prepare annual Business Continuity and Disaster Recovery plan updates and/or testing results	Collaborate with the Contractor in order to review and approve the Business Continuity and Disaster Recover plan updates and/or testing results.

Operations and Maintenance Phase: The Contractor shall conduct all activities applicable to the Operations and Maintenance Project Phase for the minimum base Contract. During this Project Phase, there shall be a Warranty Period as described in section 15.H of this Contract.
Entrance Criteria: • The entrance criterion for the System Operations and Maintenance Phase activities is Departmental acceptance of the System as operational.
Exit Criteria: • Department has notified the Contractor that the Contract will be terminated (e.g., all optional Contract extensions are exhausted or the Department chooses not to exercise an option to renew).

#	Contractor Responsibilities	Department Responsibilities
103.	Prepare an annual Business Plan for Department approval.	Collaborate with the Contractor in order to review and approve the Business Plan.
104.	Develop a System Operational Procedures Manual.	Collaborate with the Contractor in order to review and approve the System Operational Procedures Manual.
105.	Perform operations and maintenance throughout the life of the Contract at no additional cost to the Department, and develop and make available electronically a System Operations and Maintenance Plan.	Collaborate with the Contractor in order to review and approve the System Operations and Maintenance Plan and provide guidance where appropriate.

#	Contractor Responsibilities	Department Responsibilities
106.	Provide twenty-four (24)/seven (7) live pharmacy Help Desk support through a toll-free number for Department and authorized users. Authorized users shall be allowed to leave a voicemail if the help desk agent is busy. The help desk shall be primarily responsible for the following activities: a. Performing initial investigation, impact assessment, and prioritization on all requests. b. Handling routine requests such as user ID, password, and security profile issues. c. Forwarding non-System related issues to the appropriate Department or Contractor staff. d. Escalating issues as defined in the Operations and Maintenance Plan. e. Capturing and tracking helpdesk requests (i.e., tickets) and reporting resolutions back to the end-user.	
107.	Prioritize and resolve issues coming into the pharmacy Help Desk using mutually agreed upon Severity definitions. The Department reserves the right to determine and assign levels of severity for the issue/support problems. The severity of the issue/support problem shall determine the problem resolution response time.	Review regular operations reports and assist the Contractor in assigning severity levels to reported issues.
108.	Provide help desk support during key business hours and non-key business hours support, as defined in the System Operations and Maintenance Plan.	

#	Contractor Responsibilities	Department Responsibilities
109.	Continuously monitor for issues/defects and correct defects identified by the Department and/or Contractor.	Inform the Contractor of all issues/defects.
110.	Offer recommendations to the Department on any improvements or efficiencies related to System.	Review recommendations from the Contractor and provide guidance.
111.	Participate and provide data and support to the Department and any QA/IV&V Contractors.	
112.	Publish a System Software Version Release Schedule and provide updates to the Department as requested.	Review System Software Version Release Schedule.
113.	Utilize the approved Project Control and Issue Tracking Tool, to collect and track reported issues and resolutions. The tool shall capture, at minimum, all applicable information about the issue and caller, including date of contact, name of individual making contact, organization/department name/work unit (if applicable), phone number and email address, description of problem/complaint, description of any follow up investigation/resolution plans, including the date and time of return calls, and any problem report numbers assigned or related to contact. The Contractor shall provide appropriate Department personnel with access to the tool.	Review, approve, and provide feedback on reported issues and resolutions.
114.	Provide regular reports on issues/defects and their resolutions, as defined in the Department-approved System Operations and Maintenance Plan.	Monitor Contractor and System performance for accuracy and timeliness.
115.	Provide online end user and System Administrative Documentation.	Review and approve the System Administrative Documentation.

#	Contractor Responsibilities	Department Responsibilities
116.	Ensure electronic exchange of information is secure and encrypted for the Department to report problems, questions or System issues while safely exchanging PHI/PII, as required.	Utilize the encrypted electronic exchange of information to report problems, questions, or System issues to the Contractor.
117.	Provide a searchable library, with highly flexible search criteria to enable a user to quickly find needed information in policy manuals, training material, implementation memos, etc. and all help functions.	Review and approve the searchable library.
118.	Manage and maintain up-to-date upgrades and site licenses, as covered by maintenance agreements, for software and operating systems, and provide training as Department defined.	
119.	Review progress and compliance with Operations and Maintenance Phase entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance with Operations and Maintenance Phase entrance and exit criteria.
120.	Develop and submit all Operations and Maintenance Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Operations and Maintenance Phase Deliverables and provide the Contractor with necessary access to documentation to complete the Operations and Maintenance Phase Deliverables.

CMS Certification Phase: This Project Phase includes the Contractor's support of the CMS Certification process, which includes preparing for and demonstrating that CMS Certification standards are met. The Contractor shall ensure that the PBMS will meet CMS Certification approval for the maximum allowable Federal Financial Participation (FFP) and achieve CMS Certification.
Entrance Criteria: • Resolution of all agreed upon System issues/fixes identified by the Department in its comprehensive evaluation of the System.
Exit Criteria: • The exit criterion for the CMS Certification activities is the Department receives CMS certification of the PBMS component of the MMIS enterprise or the entire MMIS enterprise, which includes the PBMS.

#	Contractor Responsibilities	Department Responsibilities
121.	Participate in CMS certification activities, as directed by the Department and its System Integrator.	• Communicate certification process and schedule, including support required by the Contractor. • Act as the liaison between CMS and the Contractor.
122.	Coordinate with the Department to develop CMS Certification Checklist documentation.	Communicate CMS Certification requirements required for the CMS Certification Checklist.
123.	Assist the Department in preparing certification documents and reports, as directed by the Department.	
124.	Provide necessary resources to the Department to support the CMS Certification, as defined by the Department.	
125.	Review progress and compliance with CMS Certification Phase entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance with CMS Certification Phase entrance and exit criteria.

#	Contractor Responsibilities	Department Responsibilities
126.	Develop and submit the CMS Certification Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all CMS Certification Phase Deliverables and provide the Contractor with necessary access to documentation to complete the CMS Certification Phase Deliverables.

Enhancements Phase: The Contractor shall work with the Department to identify, prioritize, plan, define, develop, test, and implement changes or enhancements to the base release. The Department and Contractor will agree to Enhancements through the Change Management Process. Enhancements are defined as changes to the System functionality outside of the contracted scope, and shall require a Change Request, as defined in the Change Management Plan in Exhibit C, Requirements.
Entrance Criteria: • The entrance criterion for the Enhancements Phase activities is the Department receives CMS certification of the PBMS component of the MMIS enterprise or the entire MMIS enterprise, which includes the PBMS.
Exit Criteria: • The exit criterion for the Enhancements activities is the Department approval of the Enhancements activities.

#	Contractor Responsibilities	Department Responsibilities
127.	Collaborate with the Department to identify and prioritize its System requirements that are not included in the base System and are outside of the contracted scope, following the Change Management Process.	• Provide the appropriate staff to work with the Contractor to identify and prioritize System enhancements. • Collaborate with the Contractor in order to review and approve the Enhancements Requirements Change Order.
128.	Configure the System per approved design specifications to meet the Enhancement Requirements.	
129.	As necessary, conduct walkthroughs of System enhancements for the Department.	Provide the appropriate staff to attend System enhancement walkthroughs.
130.	Develop an Enhancements Test Plan that describes the approach to all testing necessary to implement the enhancements.	Review and approve the Enhancements Test Plan.

#	Contractor Responsibilities	Department Responsibilities
131.	Provide all tools used to facilitate the testing process, including performance testing. The Department will not procure testing tools for this project and any testing tools proposed shall be provided by the Contractor and licensed by the Contractor for use by its staff and the applicable Department staff for the project at the testing site.	
132.	Provide any required training on the proposed testing tools to all Department staff that will be required to use these tools.	Identify and schedule training for Department staff.
133.	Design, implement, and document detailed Test Cases for enhancement testing.	• Approve all Test Cases prior to testing and reserve the right to request that additional Test Cases be developed and tested. • Provide the necessary Department resources to participate in UAT.
134.	Ensure all testing, issue resolution, and code promotion activities maintain zero impact to Department day-to-day operations. Submit all Test Results for each test sub-phase to the Department.	• Review, approve, and provide feedback on the final Enhancements Test Results. • Inform Contractor of any impact(s) to day-to-day operations.
135.	Provide the Department with testing progress, as part of the weekly status reports including, at minimum: • The number of issues identified. • Type. • Severity. • Mitigation strategy. • Projected resolution date.	• Review and approve Contractor documentation that all System required data is transferred and functions according to Colorado specifications. • Act as mediator to resolve any System installation problems. • Review and approve System modifications or miscellaneous documentation made by the Contractor during the Enhancements Phase.

#	Contractor Responsibilities	Department Responsibilities
136.	Implement System enhancements.	
137.	Review progress and compliance with Enhancements Phase entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance Enhancements Phase entrance and exit criteria.
138.	Develop and submit the Enhancements Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Enhancements Phase Deliverables and provide the Contractor with necessary access to documentation to complete the Enhancements Phase Deliverables.

Turnover Phase: The Contractor may be required to transition operations of the System, at no additional cost to the Department or a new contractor, at the end of the Contract term. The primary activities in this Project Phase are focused on transition planning to ensure operational readiness for the Department and/or new contractor. This includes both a knowledge transfer period, and actual System turnover to the Department and/or new contractor. The Department shall sign-off on each defined Milestone to ensure that all Deliverables and exit criteria are fully executed based on agreed upon Contract terms. The Department will act as the Contractor's liaison to ensure participation from all parties during the Turnover Phase.
Entrance Criteria: • The entrance criterion for the Turnover Phase activities is a complete set of criteria for conducting turnover activities. • The Department has given notice that it intends to enter the Turnover Phase.
Exit Criteria: • Department acceptance of Turnover Phase activities.

#	Contractor Responsibilities	Department Responsibilities
139.	Designate a staff member as the Turnover Coordinator. This individual shall become a full-time Turnover Coordinator until termination of the Contract upon initiation of the Turnover Phase.	
140.	Develop a System Turnover Plan at no additional cost to the Department.	• Communicate turnover process and schedule, including support required by the Contractor. • Act as the liaison between legacy Contractor and the replacement Contractor. • Collaborate with the Contractor in order to review and approve the System Turnover Plan.

#	Contractor Responsibilities	Department Responsibilities
141.	Develop a System Requirements Statement at no extra cost that would be required by the Department or another designee to fully take over System, technical, and business functions outlined in the Contract(s).	• Communicate the turnover requirements required for the completion of a successful Turnover Phase. • Review and approve the System Requirements Statement.
142.	Provide Turnover Services, including, at minimum: a. A copy of the operational System(s) on media as determined by the Department. b. Documentation, in an editable format, including, all relevant System manuals needed to maintain and operate the System. c. Onsite System training and knowledge transfer for Department/new Contractor staff, as determined by the Department.	
143.	Provide a Lessons Learned Document that describes valuable lessons learned during the COMMIT project.	Review the Lessons Learned Document.
144.	Review progress and compliance with Turnover Phase entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance Turnover Phase entrance and exit criteria.
145.	Develop and submit the Turnover Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Turnover Phase Deliverables and provide the Contractor with necessary access to documentation to complete the Turnover Phase Deliverables.

PBMS Operations:

The following tables apply to the PBMS Operations. These tables reflect the responsibilities of the Contractor and the Department in operating the federally certified System. As opposed to the preceding tables, which described the development, Configuration, testing, and certification of the System, these tables describe the activities necessary for the Department to make the transition from the incumbent contractor to the Contractor in order to fully operate and maintain the PBMS.

PBMS Operations Transition Planning: The Contractor shall lead the transition planning effort on behalf of the Department. Transition planning shall begin at the start of the Testing Project Phase and continue through the Implementation and Rollout Project Phase. The Contractor shall plan and facilitate discussions among stakeholders in the transition including the Department and the incumbent Fiscal Agent to make certain that all relevant activities and Milestones are captured in the Transition Plan. The Contractor shall be responsible for development of the Transition Plan, consolidation of relevant sections of the incumbent Fiscal Agent's Turnover Plan into the Contractor's Transition Plan, and maintenance of the consolidated Transition Plan, as detailed in Exhibit C, Requirements.
Entrance Criteria: • Department approval of the Contractor's Detailed Project Plan. • Establishment of a location where Contractor operations and services will be performed.
Exit Criteria: • Department acceptance of the Contractor's Transition Plan. • Department acceptance of the Contractor's Relocation Risk/Contingency Plan.

#	Contractor Responsibilities	Department Responsibilities
146.	Select and establish a Contractor operations site per the requirements in the Exhibit C, Requirements.	Approve the Contractor operations site.
147.	Conduct a review of the current Systems and user documentation, and clarify deficiencies as necessary.	Provide the Contractor current Systems and user documentation.

#	Contractor Responsibilities	Department Responsibilities
148.	Develop and submit a Transition Plan.	Collaborate with the Contractor in order to review and approve the Transition Plan.
149.	Develop and submit a Relocation Risk/Contingency Plan.	Collaborate with the Contractor in order to review and approve the Relocation Risk/Contingency Plan.
150.	Develop and establish the gateway to the Department's LAN to facilitate communications between the Department and the Contractor, and supply all hardware and software needed to properly establish communications.	
151.	Acquire necessary hardware and software needed for a successful transition including any current Contractor hardware and software owned by the Department.	
152.	Plan, facilitate and document Transition Planning meetings involving the Department and prior Contractor to identify and document details related to transitioning operational responsibilities, stored data/documentation, and applicable hardware/software.	• Coordinate communication, and act as liaison between the new Contractor and the incumbent. • Provide the new Contractor with all available documentation on current Contractor operations and Colorado requirements. • Provide the new Contractor with final schedules published by the current Contractor for all cycle processes. • Coordinate the transition of Department-owned property (i.e., office furniture, equipment, hardware and software) to the new Contractor, termination, or assumption of leases of System hardware and software.
153.	Review progress and compliance with Transition Planning entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance Transition Planning entrance and exit criteria.

#	Contractor Responsibilities	Department Responsibilities
154.	Develop and submit the Transition Planning Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Transition Planning Deliverables and provide the Contractor with necessary access to documentation to complete the Transition Planning Deliverables.

PBMS Operations Parallel Testing: The Contractor shall demonstrate that the System is fully ready for operations. During PBMS Operations Parallel Testing, the Contractor will utilize input files from the incumbent Fiscal Agent's claims processing activities and compare the output results to determine data integrity of the System. The Contractor shall be responsible for running prior cycles of standardized reports from the System to compare to reports from the Legacy System.
Entrance Criteria: • Department approval of the Contractor's Development and Testing.
Exit Criteria: • Department approval of Parallel testing results.

#	Contractor Responsibilities	Department Responsibilities
155.	Establish an Operations Parallel Test Plan that describes the Contractor's approach to conducting the parallel test.	Identify and coordinate with appropriate Department staff and the incumbent to provide testing data to cover the breadth and volume of the System.
156.	Develop procedures and supporting documentation for parallel testing.	Review and approve procedures and supporting documentation for parallel testing.
157.	Establish a parallel test schedule in coordination with the Department and incumbent.	Collaborate with the Contractor to review and approve the parallel test schedule.
158.	Perform parallel test of the new Contractor with input from the incumbent Contractor's operations and report test results to the Department.	Provide oversight and formal acceptance of the Parallel Test Results.
159.	Identify and generate test data, as needed.	Approve test data, as needed.
160.	Revise System and user documentation as required to fully describe the new Contractor's operations.	Review and approve revised System and user documentation.

#	Contractor Responsibilities	Department Responsibilities
161.	Work with other System Contractor(s) and the Department to establish and ensure appropriate System and business interfaces as deemed necessary by the Department to successfully meet the responsibilities identified for Parallel Testing.	Collaborate with the Contractor to establish and ensure appropriate System and business interfaces.
162.	Review progress and compliance with Parallel Test entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance with Parallel Test entrance and exit criteria.
163.	Develop and submit the Parallel Test Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Parallel Test Deliverables and provide the Contractor with necessary access to documentation to complete the Parallel Test Deliverables.

PBMS Operational Readiness: The Contractor shall perform specific implementation and PBMS operations functions to ensure operational readiness. In preparation for operations, the Contractor will perform final file conversions, recruit, and train operations staff, and conduct any necessary provider and Department staff training.
Entrance Criteria: • Department acceptance of the Parallel Test.
Exit Criteria: • Department acceptance of the Operational Readiness Assessment.

#	Contractor Responsibilities	Department Responsibilities
164.	Modify operating procedures to reflect changes with Contractor PBMS Operations.	Review and approve the revised Operating Procedures.
165.	Develop or revise provider manuals to reflect changes with Contractor PBMS Operations.	Review and approve the revised Provider Manuals.
166.	Submit an updated Resource Management Plan for Contractor operations.	Review and approve updated Resource Management Plan for Contractor PBMS Operations.
167.	Revise the report distribution schedule to reflect updated Department decisions on format, media, and distribution.	
168.	Coordinate and schedule Contractor training from Department to ensure that Contractor staff is adequately educated in Colorado policies and existing Systems.	• Collaborate with the Contractor to finalize a training schedule for System user trainings. • Provide the Contractor with program, policy and existing System/tool training as appropriate. • Coordinate the necessary Department staff to conduct Contractor training sessions.

#	Contractor Responsibilities	Department Responsibilities
169.	Conduct orientation and training for Department personnel on Contractor organization, functional responsibilities, and operational procedures.	Provide staff time to attend training sessions conducted by the Contractor for Department personnel.
170.	Develop a Provider Transition Training Plan, and conduct any necessary provider training sessions.	• Approve notices to be sent to providers regarding transition issues and the process. • Collaborate with the Contractor in order to review and approve the Provider Transition Training Plan.
171.	Develop a Department Operational Readiness Training Plan and conduct training for Department staff in order to ensure preparedness for operations	Collaborate with the Contractor in order to review and approve the Department Operational Readiness Training Plan.
172.	Conduct a formal Operational Readiness Plan Walkthrough with the Department, demonstrating that all operational areas are ready.	Participate in and provide feedback regarding the formal Operational Readiness Plan Walkthrough.
173.	Prepare a final Operational Readiness Assessment Document, including results of the parallel test and an assessment of the final operational readiness of new Contractor.	Collaborate with the Contractor in order to review and approve the final Operational Readiness Assessment Document.
174.	Review progress and compliance with Operational Readiness Phase entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance with Operational Readiness Phase entrance and exit criteria.
175.	Develop and submit the Operational Readiness Phase Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Operational Readiness Phase Deliverables and provide the Contractor with necessary access to documentation to complete the Operational Readiness Phase Deliverables.

PBMS Operations Implementation and Start of Operations: The Contractor shall be responsible for ensuring a successful implementation of the System and PBMS Operations that minimizes, to the greatest practical extent, negative impact on the Department and its authorized users.
Entrance Criteria: • Department acceptance of the Operational Readiness Assessment.
Exit Criteria: • Attestation from Contractor that System is operation-ready.

#	Contractor Responsibilities	Department Responsibilities
176.	Conduct any additional orientation and training for Department personnel on Contractor organization, functional responsibilities, and operational procedures.	Provide staff time to attend training sessions conducted by the Contractor for Department personnel.
177.	Conduct any necessary provider or Department training sessions.	Provide staff time to attend training sessions conducted by the Contractor for Department personnel.
178.	Make arrangements for the acceptance of all claim-related receipts and pending claims from the incumbent Contractor for completion of processing after cutover. No new claims, in electronic format or hard copy, shall be accepted by the incumbent Contactor during the final five (5) Business Days prior to the transfer date.	Work with incumbent Contractor on remaining turnover tasks.
179.	Allow for the complete resolution of all edits and adjudication of claims by the incumbent Contractor to be transferred.	

#	Contractor Responsibilities	Department Responsibilities
180.	Perform final conversion and review conversion reports to demonstrate successful conversion.	
181.	Implement all network connectivity and communications.	Coordinate the termination or assumption of leases of appropriate hardware and software, where appropriate.
182.	Provide attestation to the Department that the System is operation-ready.	Approve attestation from Contractor that System is operation-ready.
183.	Review progress and compliance with Implementation and Start of Operations entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance with Implementation and Start of Operations entrance and exit criteria.
184.	Develop and submit the Implementation and Start of Operations Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all Implementation and Start of Operations Deliverables and provide the Contractor with necessary access to documentation to complete the Implementation and Start of Operations Deliverables.

PBMS Operations: The Contractor shall be expected to meet the responsibilities, Milestones, Deliverables, and performance expectations included in this Contract to ensure the successful implementation of the System with minimal disruption to clients, providers, and Department staff. The Department will work with the Contractor to establish a specific date in which the Contractor will be responsible for processing claims. Any changes to requirements subsequent to the Effective Date will be handled via the Change Management Process.
Entrance Criteria: • Department approval of the Contractor's Operational Readiness Assessment. • Attestation from Contractor that System is operation-ready. • Department approval of provider manuals. • Department approval of revised operations procedures.
Exit Criteria: • Department Intent to turn over operation to the State or another Contractor.

#	Contractor Responsibilities	Department Responsibilities
185.	Perform all Operational and Maintenance functions as defined in the Exhibit C, Requirements (Contractor Operations).	• Serve as a liaison between the Contractor and other agencies and/or Federal agency representatives. Provide QA and oversight of System functionality to ensure Colorado Medical Assistance program business needs are met and to ensure operational performance. • Review and approve Modification/Change Request Forms. • Review and approve Requirements Specifications for Approved Change Requests. • Prepare and submit to the Contractor a written change request for Department-initiated modifications.

#	Contractor Responsibilities	Department Responsibilities
186.	Perform all operational and maintenance functions as defined in the Exhibit C, Requirements (Contractor Operations).	• Monitor System modification activities. • Participate in acceptance testing of modifications in a partnership with the Contractor. • Approve implementation of a modification prior to its installation in the production System environment. • Initiate, or review and follow up on, operations problem reports. • Monitor the resolution of problems identified by the Contractor or Department staff. • Notify the Contractor of performance problems, providing written notification of failures to meet performance requirements.

#	Contractor Responsibilities	Department Responsibilities
187.	Perform all operational and maintenance functions as defined in the Exhibit C, Requirements (Contractor Operations).	• Monitor the Contractor's systems work and systems performance for accuracy and timeliness. • Review and approve updates to System documentation. • Review and approve updates to user documentation and operations procedures (if required). • Review and approve Monthly Reports on System Operation and Performance. • Review Updated Procedures and System Documentation, as needed. • Review and approve the Systems Operations Procedure Manual annual updates. • Determine priority of change requests and monitor System modification activities. • Assist the Contractor in conducting a detailed requirements analysis on any major changes as required.
188.	Ensure all maintenance, upgrades, and enhancements to the System are implemented by the deadlines coordinated with the Department.	Collaborate with the Contractor to implement and enforce deadlines for all maintenance, upgrades, and enhancements to the System.
189.	Provide support staff for the Call Center and Help Desk as defined in the Exhibit C, Requirements. Multi-lingual and translation services shall be supported during these time frames.	
190.	Respond to and resolve issues and requests received through the Call Center and Help Desk in accordance with the agreed upon response and resolution schedule.	

#	Contractor Responsibilities	Department Responsibilities
191.	Immediately notify appropriate Department staff of any technical issues discovered while researching problems reported to the Call Center and Help Desk that directly impact continuity of business operations.	Review technical issues discovered by the Contractor.
192.	Ensure Contractor staff remains up to date on all operation and functional aspects of the Department and System, including user manuals, billing manuals, resolution manuals and other reference documentation.	
193.	Provide the capability to contact the Call Center and Help Desk via phone, email, and Web Portal generated interactive sessions.	
194.	Obtain approval from the Department of all documentation and material prior to publication and distribution.	Approve all documentation and material prior to publication and distribution.
195.	Ensure all Call Center and Help Desk staff are trained in billing procedures, current Colorado Medical Assistance program policy, and telephone etiquette.	
196.	Provide for periodic training of telephone representatives. This should also include initial training for any new representatives and regular training whenever there is a change to the System or to Colorado Medical Assistance program policy.	
197.	Provide a mail drop box for Provider claims delivered directly to the Contractor.	
198.	Comply with United States Postal Service standards.	

#	Contractor Responsibilities	Department Responsibilities
199.	Maintain a claims inventory and control process.	
200.	Establish inventory controls to ensure proper accounting for all mail, claims, tapes, diskettes, cash, checks, or any other deliveries.	
201.	Return to Providers those paper claims not passing basic data content edit criteria and other situations or conditions defined by the Department, and maintain a log to track returned claims.	
202.	Identify and reprocess all claims and adjustments with errors due to errors caused by individuals or System malfunction caused by the Contractor. These transactions shall be separately reported in claims processing statistics.	
203.	Review progress and compliance with PBMS Operations entrance and exit criterion as agreed upon by the Contractor and Department.	Review progress and compliance with PBMS Operations entrance and exit criteria.
204.	Develop and submit the PBMS Operations Deliverables detailed in Exhibit C, Requirements in accordance with the Department's schedule.	Review all PBMS Operations Deliverables and provide the Contractor with necessary access to documentation to complete PBMS Operations Deliverables.

EXHIBIT E, COMPENSATION AND QUALITY MAINTENANCE PAYMENTS

1. BASE COMPENSATION AND PAYMENTS

1.1. Compensation

1.1.1. The Department shall pay the Contractor the following Monthly Contract Stage Payment amounts, as described in this section:

1.1.1.1. Monthly Contract Stage Payment Table:

Contract Stage	Monthly Contract Stage Payment Amount	Maximum Number of Monthly Payments	Stage Maximum Payment Amount*
PBMS Implementation Contract Stage	$553,846.15 (with $478,846.15 due for October 2015 and October 2016)	13	$7,049,999.95
PBMS Ongoing Operations and Enhancement Contract Stage – Year 1 (SFY2016-17)	$237,500.00	8	$1,900,000.00
PBMS Ongoing Operations and Enhancement Contract Stage – Year 2 (SFY2017-18)	$237,500.00 (with $162,500.00 due for October 2017)	12	$2,775,000.00
PBMS Ongoing Operations and Enhancement Contract Stage – Year 3 (SFY2018-19)	$237,500.00 (with $162,500.00 due for October 2018)	12	$2,775,000.00
PBMS Ongoing Operations and Enhancement Contract Stage – Year 4 (SFY2019-20)	$237,500.00 (with $162,500.00 due for October 2019)	12	$2,775,000.00
PBMS Ongoing Operations and Enhancement Contract Stage – Year 5 (SFY2020-21)	$237,500.00 (with $162,500.00 due for October 2020)	12	$2,775,000.00
PBMS Ongoing Operations and Enhancement Contract	$237,500.00 (with $162,500.00 due for October 2021)	12	$2,775,000.00

Stage – Year 6 (SFY2021-22)			
PBMS Ongoing Operations and Enhancement Contract Stage – Year 7 (SFY2022-23)	$237,500.00 (with $162,500.00 due for October 2022)	12	$2,775,000.00
PBMS Ongoing Operations and Enhancement Contract Stage – Year 8 (SFY2023-24)	$237,500.00 (with $162,500.00 due for October 2023)	4	$875,000.00
*Does not include Quality Maintenance Payment or postage. Includes reduction of $75,000.00 each October as described in Section 1.1.1.2.4			

1.1.1.2. The Department shall make a Monthly Contract Stage Payment to the Contractor for each Contract Stage for each month during that Contract Stage. If any Stage begins on a day that is not the first day of the month, then for any such month, the Department shall pay the Contractor a prorated portion of the monthly payment equal to the portion of days in the month following the beginning of the stage to the total number of days in that month. If the Department pays a prorated portion of a month at the start of any Contract Stage, then that Contract Stage shall end on a day that is not the end of a month and the final payment for that stage shall be for the remaining monthly amount less the prorated portion already paid at the beginning.

1.1.1.2.1. In the event that the Contractor completes all requirements for the PBMS Implementation Contract Stage prior to the expected completion date of that stage as shown by the Maximum Number of Monthly Payments column in the table in this section, the Department shall continue to make Monthly Contract Stage Payments to the Contractor for that stage until the Stage Maximum Payment Amount for that stage is reached. The Department may, in its sole discretion, choose to continue making monthly payments in such a circumstance or may choose to make one or more lump-sum payments for that stage that includes amounts for multiple future Monthly Contract Stage Payments for that stage.

1.1.1.2.2. In the event that the Contractor fails to meet all requirements for the PBMS Implementation Contract Stage by the expected completion date of that stage as shown by the Maximum Number of Monthly Payments column in the table in this section, the Contractor shall continue to perform all Work related to that stage and shall complete all requirements of that stage, but the Department shall not make any additional payment to the Contractor for that stage. In no event shall the Department make any Monthly Contract Stage payment to the Contractor for a stage that exceeds the Stage Maximum Payment Amount for that stage.

1.1.1.2.3. Notwithstanding anything to the contrary elsewhere in this Contract, in the event that the Effective Date is earlier than October 1, 2015, the Contractor shall not earn a Monthly Contract Stage Payment for any month prior to October of 2015. In this event, the Contractor shall receive all Monthly Contract Stage

Payments for the PBMS Implementation Contract Stage in the same manner as it would have if the Effective Date had been October 1, 2015.

1.1.1.2.4. Because the Department will be providing its own FDB license in accordance with Exhibit C, Section 34.2.3., the Monthly Contract Stage Payment for October of each SFY shall be reduced by seventy-five thousand dollars ($75,000.00).

1.1.1.3. All license fees paid to the Contractor are included in the Monthly Contract Stage Payment Amount described above. The following table shows the number of available licenses and the price per license for reference, but the Department shall not make any additional payment for any licenses shown in this table.

1.1.1.3.1. License Table:

License Description	Number of Licenses	Price per License	Total Price for all Licenses
Cognos Power Users	25	$2,225.00	$55,625.00
Cognos Consumer Users	25	$230.00	$5,750.00
Citrix User License	25	$500.00	$12,500.00

1.1.1.3.2. Not included in the Contractor's licensing to the State are the following applications, licenses held by the Contractor for which the Contractor is not receiving additional payment, and which are part of the shared infrastructure being leveraged for the CO PBMS:

1.1.1.3.2.1. FirstRx™

1.1.1.3.2.2. FirstTrax™

1.1.1.3.2.3. eRebate™

1.1.1.3.2.4. All other, shared services infrastructure software on which the PBM solutions will be running, such as the following:

1.1.1.3.2.4.1. Cognos Server Software

1.1.1.3.2.4.2. Operating System Software

1.1.1.3.2.4.3. Enterprise Service Bus Software

1.1.1.3.2.4.4. Application Server Software

1.1.1.3.2.4.5. Informatica ETL Software

1.1.1.3.2.4.6. Citrix Server Software

1.1.1.3.2.4.7. Database Server Software including but not limited to Oracle and MS SQL Server

1.1.1.3.3. The Contractor shall provide all licenses described in the License Table in this section 1.1.1.3.1.

1.1.1.3.3.1. In the event that the name of a license contained in the License Table changes, but otherwise contains the same functionality, the Parties may

agree to use that new name through a transmittal without a formal amendment to this Contract.

1.1.1.3.4. In the event that the Contractor requires additional licenses for its own staff to meet any requirement listed in this Contract, the Contractor shall provide all such licenses necessary to meet the requirements of this Contract at no additional cost to the Department. This shall not apply to additional licenses required for Department staff use or required based on incorrect information provided by the Department. This shall also not apply to additional licenses needed as a result of the addition of requirements through an amendment to this Contract, and the need for all such additional licenses resulting from requirements added through an amendment shall be negotiated as a part of that amendment.

1.1.1.4. The Contractor shall break out payment components on its invoice as directed by the Department and to provide information necessary for the Department to get enhanced federal funding.

1.1.2. The Department shall reimburse the Contractor for all actual postage costs expended by the Contractor during a month, up-to the Maximum Annual Pass-Through Postage Amount shown in the Maximum Pass-Through Postage Table for each SFY.

1.1.2.1. Maximum Pass-Through Postage Table

State Fiscal Year	**Maximum Annual Pass-Through Postage Amount**
SFY 2016-17 (July 1 2016-June 30 2017)	$0.00
SFY 2017-18 (July 1 2017-June 30 2018)	$0.00
SFY 2018-19 (July 1 2018-June 30 2019)	$0.00
SFY 2019-20 (July 1 2019-June 30 2020)	$0.00
SFY 2020-21 (July 1 2020-June 30 2021)	$0.00
SFY 2021-22 (July 1 2021-June 30 2022)	$0.00
SFY 2022-23 (July 1 2022-June 30 2023)	$0.00
SFY 2023-24 (July 1 2023-Oct 31 2023)	$0.00

1.1.2.2. The Contractor shall attempt to use the least expensive postage available for each mailing necessary to comply with all requirements of this Contract related to that mailing.

1.1.2.3. In the event that the postage costs for a year will exceed the amount shown in this section, the Contractor shall not be required to make any mailing that will result in payment of postage that exceeds the amounts shown in this section. The Department may increase this pass-through postage amount maximum through the use of an Option Letter.

1.1.2.4. Postage fulfillment will be provided by third-party shipping agents or US Postal Service. Contractor will act in the capacity of an agent role for postage fulfillment and is not liable for non-delivery except as a result of mislabeling of material by Contractor.

1.1.2.4.1. Contractor will be paid for its services pursuant to Exhibit E, including postage, for any non-delivery by third-parties or the US Postal Service;

1.1.2.4.2. Contractor will be paid for any reshipments/second mailings required due to mis-delivery by third parties;

1.1.2.4.3. Contractor will invoice postage as a separate line item on monthly invoices for regular fixed and variable fees

1.1.2.4.4. If non-delivery was a result of mislabeling of material by Contractor, the Contractor will reship or provide second and subsequent mailings at no cost for its services or postage.

1.1.2.4.5. Allowable postage costs will be reimbursed as an additional pass through (cost based) charge to the Department.

1.1.3. Enhancement Projects

1.1.3.1. Enhancement Project Rate Table

Enhancement Project Position	**Base Hourly Rate**
Configuration Staff	$70.00
Customization Staff	$90.00
Testing and Validation Staff	$60.00
Business Analyst Staff	$70.00
Technical Writing and System Documentation Staff	$55.00
Project Management Staff	$85.00

1.1.3.2. The Department shall pay the Contractor for each Enhancement project for the hours described in the Department-approved requirements for that Enhancement project.

1.1.3.3. All Enhancement project hours shall be paid based on the rates as follows:

1.1.3.3.1. The base hourly rates shown in the Enhancement Project Rate Table above are valid for SFY 2016-17.

1.1.3.3.2. For each SFY after SFY 2016-17, the base hourly rate shall increase by three percent (3%) per SFY.

1.1.3.4. The Base Hourly Rate shall apply to hours actually expended directly on the Enhancement project work, as accounted for by the Contractor.

1.1.4. Multistate Initiatives

1.1.4.1. The Contractor shall review new PBMS capabilities implemented for other states with the Department for potential inclusion in the Colorado PBMS. In the event that there will be a cost associated with this inclusion, the Contractor shall provide an estimate for implementing capabilities from other states into the Colorado PBMS as requested by the Department. If required, the Department will obtain agreement from the affected state.

1.1.4.2. If the Department decides to participate in a multi-state collaborative PBMS development initiative, the Department may have to pay a fee representing its share of the common development expenses. The Contractor shall then provide an estimate for implementing the collaborative-sponsored capability into the Colorado PBMS as requested by the Department.

2. QUALITY MAINTENANCE PAYMENTS & PERFORMANCE STANDARDS

2.1.1. The Department shall pay the Contractor the following Quality Maintenance Payments (QMPs), as described in this section:

2.1.1.1. One-Time DDI QMPs

2.1.1.1.1. One-Time DDI QMP Table

DDI QMP Name	DDI QMP Amount
PBMS Implementation Contract Stage QMP	$560,000.05
CMS Certification QMP	$240,000.00

2.1.1.1.2. The Contractor may earn the amounts shown in the One-Time DDI QMP Table as follows:

2.1.1.1.2.1. DDI QMP Release Criteria

Contract Stage	QMP Release Criteria
PBMS Implementation Contract Stage	Department releases QMP after Department has accepted all deliverables and determined the Contractor has meet all requirements for the PBMS Implementation Contract Stage.
CMS Certification Project Phase	Department releases QMP following receipt of official CMS certification of the PBMS component of the MMIS enterprise or the entire MMIS enterprise, which includes the PBMS.

2.1.1.1.3. The Department shall pay the Contractor all One-Time DDI QMPs once those QMPs are earned by the Contractor. Once the Department has determined that the Contractor has earned a QMP, the Department will provide the Contractor with Authorization to invoice for that QMP.

2.1.1.1.4. If the Contractor believes that the Contractor is not at fault for a delay that results in the Department not making the payment of any One-Time DDI QMP, other than the CMS Certification QMP, then the Contractor may dispute the Department's decision through the Dispute Process. The Dispute Process related to the non-payment of a QMP shall not begin until at least sixty (60) Business Days have passed from when the Contractor has notified the Department in writing that the Contractor believes the delay in paying the QMP is because of circumstances beyond the Contractor's control.

2.1.1.1.4.1. The CMS Certification QMP shall only be made by the Department after the Department has officially received certification of the PBMS from CMS, regardless of any delay in receiving certification. The Contractor shall not dispute the Department's decision to not pay the CMS Certification QMP prior to the Department's official receipt of CMS's certification of the PBMS. The Department expects that the CMS Certification QMP will be paid in SFY 2016-17, but in the event that a delay in CMS's certification of the PBMS would result in the payment of that

QMP being made in a later SFY, the Parties will amend the Contract accordingly.

2.1.1.2. Quality Maintenance Payment—PBMS Ongoing Operations and Enhancements Contract Stages

2.1.1.2.1. The Contractor may earn an Ongoing Operations QMP for a month for each performance standard listed in the Ongoing Operations QMP Table shown below that the Contractor meets or exceeds during that month. If the Contractor fails to meet or exceed a performance standard listed in the Ongoing Operations QMP Table during a month, then the Contractor shall not earn an Ongoing Operations QMP for that performance standard for that month.

2.1.1.2.2. A QMP shall be applied to all of the performance standards and requirements listed in this section. Some of these performance standards duplicate performance standards contained in Exhibit G. For each standard from Exhibit G, the Contractor shall comply with the associated requirement in Exhibit C as part of its compliance with the performance standard in this section in order to earn a QMP for that performance standard.

2.1.1.2.3. During the first one-hundred and eighty (180) calendar days of the first year of the PBMS Ongoing Operations and Enhancement Contract Stage, the Department may make a QMP for a performance standard, even if the Contractor has not met the performance standard for that QMP, at the Department's discretion.

2.1.1.2.4. The following table shows the QMP allocation to each of the performance standards. The Contractor shall earn the listed QMP for a performance standard for each month during any annual PBMS Ongoing Operations and Enhancement Contract Stage that the Contractor meets or exceeds that performance standard.

2.1.1.2.4.1. The Contractor may only earn the QMP for each performance standard once during a month, and in no event shall the total of all QMPs for a month exceed the QMP total shown in the following table for the PBMS Ongoing Operations and Enhancement Contract Stage Year in which the month occurs:

2.1.1.2.4.1.1. Ongoing Operations QMP Performance Standards Table

Performance Standard	PBMS Ongoing Operations and Enhancement Contract Stage – Year 1 Monthly QMP	PBMS Ongoing Operations and Enhancement Contract Stage – Year 2 Monthly QMP	PBMS Ongoing Operations and Enhancement Contract Stage – Year 3 Monthly QMP	PBMS Ongoing Operations and Enhancement Contract Stage – Year 4 Monthly QMP	PBMS Ongoing Operations and Enhancement Contract Stage – Year 5 Monthly QMP	PBMS Ongoing Operations and Enhancement Contract Stage – Year 6 Monthly QMP	PBMS Ongoing Operations and Enhancement Contract Stage – Year 7 Monthly QMP	PBMS Ongoing Operations and Enhancement Contract Stage – Year 8 Monthly QMP
Staff Retention and Backfill if Vacancy performance standard - The Contractor shall provide backup resources during the planning stages for training in the case that any key personnel would leave the program for any unforeseen reason. Recruiting shall begin immediately for the Pharmacy Services Account Manager and the Pharmacy Systems Manager who shall both be located at the Contractor's Denver facility.	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89
System availability performance standard – the PBMS was available to PBMS users ninety-nine and one-half percent (99.5%) of time during normal service hours each month.	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89
Claim adjudication accuracy performance standard - 99.9% of all claims were processed with no errors each month.	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89
Business Continuity Performance Standard - • No mission critical services (priority 1 as described in the Business Continuity and Disaster Recovery Plan) were interrupted during the month.	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89

• All core services that are required to be maintained with limited service disruption (priority 2 as described in the Business Continuity and Disaster Recovery Plan) were recovered within eight (8) hours following the event that resulted in those services being unavailable -OR- no priority 2 services were interrupted during the month. • Systems and data where service disruption will cause serious injury to government operations, staff, or citizens (priority 3 as described in the Business Continuity and Disaster Recovery Plan) were all recovered within forty-eight (48) hours following any event that results in those services being unavailable -OR- no priority 3 services were interrupted during the month. • Systems and data required for moderately critical agency services and IT functions where damage to government operations, staff, and citizens would be significant but not serious (priority 4 as described in the Business Continuity and Disaster Recovery Plan) were all recovered within five (5) Business Days following any event that results in those services being unavailable -OR- no priority 4 services were interrupted during the month. • Systems and data required for less critical support systems (priority 5 as described in the Business Continuity and Disaster Recovery Plan) were all recovered on timeframe as mutually agreed upon by the Department and								

Contractor -OR- no priority 5 services were interrupted during the month... • As described in the Business Continuity and Disaster Recovery Plan, the call center was fully operational within twenty-four (24) hours following any event that caused the call center to become not operational and the alternate site was fully operational within five (5) Business Days -OR- the call center was operational at all required times during the month and the Contractor did not need to use an alternate site.								
Colorado specific staff were be available from 8:00 a.m. to 5:00 p.m. Mountain Time, each Business Day during the month. The Clinical Key Personnel were available during stated business hours during the month.	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89
Reference 2554 - The Contractor maintained a sufficient number of telephone lines, technology, and personnel so that at least ninety-five percent (95%) of all calls are answered/queued within fifteen (15) seconds, and no more than five percent (5%) of answered calls are on hold for more than one (1) minute during the month.	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89
Reference 2398 - For pharmacy claims submitted electronically by a Provider, all POS Claims were adjudicated for payment or denial within a maximum of five (5) seconds of receipt during the	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89

month. For claims submitted on paper by a Provider, all paper claims were direct data entered and adjudicated by the Contractor accurately within seventy-two (72) hours upon receipt during the month.								
100% of Prior Authorization Requests were responded to within one (1) Business Day following receipt.	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89	$1,388.89
All telephone calls and emails received from Providers were responded to within one (1) Business Day and were resolved within three (3) Business Days during the month. A response does not mean resolution is provided; instead it may include a simple acknowledgement of the inquiry or referral to another representative as long as the representative responds within the same timeframe. If the response is a referral to another representative, the response shall provide a target completion or resolution date.	$1,388.88	$1,388.88	$1,388.88	$1,388.88	$1,388.88	$1,388.88	$1,388.88	$1,388.88
Total of all Monthly QMPs	**$12,500.00**	**$12,500.00**	**$12,500.00**	**$12,500.00**	**$12,500.00**	**$12,500.00**	**$12,500.00**	**$12,500.00**

2.1.1.2.4.1.2. As mutually agreed by the Parties, any performance standards or measurement method for any performance standard listed in this table may be clarified through the use of a Transmittal. The parties may not use a Transmittal to modify the amounts of any QMP or add, modify or delete any performance standard contained herein.

3. CLARIFICATIONS

3.1. Calculations to determine if a QMP was earned shall not include:

3.1.1. Any failure to meet a performance standard that was caused by an event of Force Majeure as defined in Section 20.D, Force Majeure;

3.1.2. Any failure to meet a performance standard that was caused by a planned interruption where the Department has received prior notification; or

3.1.3. Any failure to meet a performance standard that could have been prevented through execution of a written proposal by the Contractor that was not implemented at the request of the State.

3.2. Where time measurement is required in a performance standard, the duration shall be measured from the time the Contractor knows or should know of the issue that caused the time measurement to be required through the time the Department receives notification of resolution. The calculation of any duration shall not include:

3.2.1. Time period(s) where the Contractor does not have access to a physical State location where access is necessary for problem identification and resolution; or

3.2.2. Time period(s) where the Contractor is unable to obtain necessary information from the State.

3.3. For all calculations related to QMPs, all decimals shall be rounded to two decimal places, with five and greater rounding up and four and less rounding down, unless otherwise specified.

3.4. The QMP percentage shall only be applied to a single QMP standard during any reporting period. Performance standards shall be measured in the specified reporting period and treated as pass/fail when calculated for QMP application.

3.5. QMP standards shall not be invoked for any other instance where other liquidated damages would apply.

4. PERFORMANCE STANDARD REPORTING—QMP

4.1. Each month, the Contractor shall consolidate the review findings for the QMP-related performance standards into a single report—QMP Response Summary Report. This report will list each standard with a corresponding reference number, an indicator showing the results category and the associated total QMP amount that will be invoiced.

4.2. The following are the three results categories that will be used in the QMP Response Summary Report:

4.2.1. Met-Yes—The criteria for this standard were met for the reporting period and deemed Billable/Pass.

4.2.2. Met-No—The criteria for this standard were not met for the reporting period and deemed Not Billable/Fail.

4.2.3. Waived—The Department agreed to waive the application for this standard during the reporting period because of extenuating circumstances and deemed Billable.

4.3. The Contractor shall attach the QMP Response Summary Report to the monthly invoice as documentation to support the amount of QMP claimed.

4.3.1. In addition to the QMP Response Summary Report, the Contractor shall provide necessary data, information or access for the Department to verify the information provided in the QMP Response Summary Report or the Contractor's invoice.

EXHIBIT F, TERMINOLOGY

1. TERMINOLOGY

1.1. The following list is provided to assist the reader in understanding terminology, acronyms and abbreviations used throughout this Contract.

1.1.1. Address Confidentiality Program (ACP) – The Colorado Address Confidentiality Program described in C.R.S. §24-30-2101.

1.1.2. Americans With Disabilities Act (ADA) – The Americans With Disabilities Act of 1990, 42 U.S.C. §12101 *et. seq.*

1.1.3. American Recovery and Reinvestment Act (ARRA) – The American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5.

1.1.4. Business Intelligence and Data Management (BIDM) – The contractor and system that will replace the Department's current Medicaid decision support system, Data Warehouse, and Statewide Data Analytics Contractor. As of the Effective Date of this Contract, the BIDM Contractor is Truven Health Analytics Inc.

1.1.5. Centers for Medicare and Medicaid Services (CMS) – An agency of the United States Department of Health and Human Services that provides federal oversight of the Medicaid program.

1.1.6. Change Management or Change Management Process – A process that facilitates the organized planning, development, and execution of modifications and Enhancements to the PBMS so that changes to the System are introduced in a controlled and coordinated manner, and the possibility that unnecessary changes will be introduced to a system without proper planning is reduced.

1.1.7. Change Request – A document detailing the addition or modification to the functionality of the PBMS.

1.1.8. Child Health Plan *Plus (CHP+)* – Public health insurance for children and pregnant women who earn too much to qualify for Medicaid, but cannot afford private health insurance.

1.1.9. Claim – A bill for services that is appropriate for the provider type and type of service(s), whether submitted as a paper claim or electronically, and identified by a unique claim control number. A single claim is defined as a billing comprised of a single beneficiary with the same Date of Service (or range of dates for service), submitted by a single billing provider which may include one or more service(s) or document(s).

1.1.10. Client – Any individual eligible for or enrolled in a public health insurance program administered by the Department such as the Colorado Medicaid program, Colorado's CHP+ program, the Colorado Indigent Care Program or other program as determined by the Department.

1.1.11. Colorado Benefits Management System (CBMS) – The State of Colorado's single integrated system for determining eligibility and calculating benefits for the State's major welfare programs, including Medicaid.

1.1.12. Colorado Health Benefits Exchange (COHBE) – A marketplace for Coloradans to shop for and purchase health insurance based on quality and price.

1.1.13. Colorado Operations Resource Engine (CORE) – The financial system that maintains the official accounting records for the State of Colorado government.

1.1.14. Commercial Off-The-Shelf (COTS) – A product that is sold in substantial quantities in the commercial marketplace that does not require additional software or hardware development or Customization for general use.

1.1.15. COMMIT – Colorado Medicaid Management Innovation and Transformation.

1.1.16. COMMIT Project – A project to implement and operate a new MMIS, including the implementation of the Core MMIS, the PBMS and the BIDM.

1.1.17. Configurable/Configuration – Modification of System functionality, which does not require development changes to the software and can be modified by non-technical (e.g., non-programmer or developer) staff.

1.1.18. Copayment – The Client's financial responsibility for a service, procedure or Prescription assigned by the Department.

1.1.19. Current Procedural Terminology (CPT) – A code set maintained by the American Medical Association through the CPT Editorial Panel.

1.1.20. Customer Relationship Management (CRM) – A software or system used the Contractor to organize, automate and synchronize customer service and technical support.

1.1.21. Customization – Any modification, alteration or extension to software requiring changes to the existing source code for such software to achieve new or modified functionality and that requires dedicated technical staff (e.g., a programmer or developer).

1.1.22. Dashboard – A subset of information delivery that includes the ability to publish formal, web-based reports with intuitive displays of information. It has an easy to read, often single page, real-time User Interface, showing a graphical presentation of the current status and historical trends of an organization's Key Performance Indicators to enable instantaneous and informed decisions to be made at a glance.

1.1.23. Data Dictionary – A centralized repository of information about data such as meaning, valid values, relationships to other data, origin, usage and format.

1.1.24. Data Warehouse (DW) – A database used for reporting and analysis.

1.1.25. Defect – an error, flaw, mistake, failure, or fault in a computer program or system that produces an incorrect or unexpected result that differs from an agreed-to Specification, or causes it to behave in unintended ways that differ from an agreed-to Specification..

1.1.26. Design, Development and Implementation (DDI) – The portion of the Work required to identify, design, develop and implement technical and business services.

1.1.27. Dispute Process – The process described in the Contract for the Contractor and the Department to follow to resolve all debates or disagreements between the Department and Contractor.

1.1.28. Drug Utilization Review (DUR) – A program designed to measure and assess the proper use of outpatient drugs in the Medicaid program.

1.1.29. Durable Medical Equipment (DME) – Medical equipment used in the home to aid in a better quality of living

1.1.30. Electronic Document Management System (EDMS) – Software that manages documents for electronic publishing.

1.1.31. Electronic Funds Transfer (EFT) – An electronic transfer of money, also known as direct deposit.

1.1.32. Encounter – A claim submitted by a Managed Care Entity for reporting purposes only.

1.1.33. Encounter Data – Data collected to track use of provider services by managed care health plan enrollees.

1.1.34. Enhancement – Functional changes or performance improvements that require Configuration or Customization to the System and follow the Change Management Process described in the Change Management Plan.

1.1.35. Enrolled Provider (EP) – A provider whose enrollment status is active and has billed a claim within the past twelve (12) calendar months.

1.1.36. Episodes of Care – A health problem, from its first Encounter with a health care provider through the completion of the last Encounter related to the problem, typically encompassing the patient's reason for the Encounter, the diagnosis code and the resulting therapeutic intervention.

1.1.37. Federal Financial Participation (FFP) – Federal matching funds for State expenditures relating to assistance payments for certain social services, and State medical and medical insurance expenditures.

1.1.38. Fee-For-Service (FFS) – A payment model where services are unbundled and paid for separately.

1.1.39. Fiscal Agent (FA) – An entity that acts on behalf of the State Medicaid agency in respect to claims processing, Provider Enrollment and relations, utilization review, and other functions.

1.1.40. Fiscal Year (FY) – A period used for calculating annual financial statements in businesses and other organizations.

1.1.41. Fraud – An intentional deception or misrepresentation that could result in the payment of an unauthorized benefit.

1.1.42. Full Time Equivalent (FTE) – A unit of measure that equates to the workload of an individual who works a full time schedule, regardless of the actual number of individuals who perform that work or the actual number of hours worked by those individuals.

1.1.43. Health Care Common Procedure Coding System (HCPCS) – A standardized coding system used to describe the items and services provided in health care, comprised of three levels.

1.1.44. Health Information Technology for Economic and Clinical Health Act (HITECH) - The Health Information Technology for Economic and Clinical Health Act provisions of ARRA.

1.1.45. Independent Verification and Validation (IV&V) - Processes and products to ensure adherence to Contract requirements and sound engineering practices to meet the Department's objectives.

1.1.46. Interactive Voice Response (IVR) – A technology that allows a computer to interact with humans through the use of voice and Dual-tone multi-frequency tones input via keypad.

1.1.47. International Classification of Diseases, 10th Revision, Clinical Modification (ICD-10) – The 10th revision to the International Classification of Diseases promulgated by the World Health Organization.

1.1.48. Interoperability – The ability to exchange and use information from multiple machines from multiple different entities.

1.1.49. Key Personnel – The position or positions that are specifically designated as such in this Contract.

1.1.50. Labor Category – A grouping of similar skills, knowledge, ability, experience and education specific to the labor to be provided.

1.1.51. Legacy System – The Department's existing MMIS and supporting systems as of the Effective Date, which includes PBMS functionality.

1.1.52. Maintenance – Routine activities required to sustain normal operations of the PBMS, including COTS utilized by the Contractor under this Contract and the upkeep of servers and software patches. These activities are not considered Enhancements and do not require a formal Change Management Process to complete.

1.1.53. Medicaid – The Medical assistance program authorized under Title XIX of the Social Security Act.

1.1.54. Medicaid Enterprise – The organizing logic for business processes and information technology infrastructure reflecting the integration and standardization requirements of the Colorado Medical Assistance program's operating model, which includes the MMIS.

1.1.55. Medicaid Enterprise Certification Toolkit (MECT) – A tool created by CMS to assist states in all phases of the MMIS life cycle.

1.1.56. Medicare – A health insurance program for the aged and disabled under Title XVIII of the Social Security Act.

1.1.57. Medicaid Information Technology Architecture (MITA) – A national initiative, overseen by CMS, that is intended to foster integrated business and IT transformation across the Medicaid Enterprise to improve the administration of the Medicaid program.

1.1.58. Medicaid Management Information System (MMIS) - A collection of services and automated claims processing that fulfills, at a minimum, the federal requirements specified in Part 11 of the State Medicaid Manual (CMS Publication 45), program directives and memos, policy statements, and the like that serve as the basis for CMS certification and is compliant with HIPAA requirements, as modified.

1.1.59. Milestone – A significant point, event or achievement that reflects progress toward completion of a process, phase or project.

1.1.60. National Council for Prescription Drug Programs (NCPDP) – An entity that creates and promotes standards for the transfer of data to and from the pharmacy services sector of the health care industry.

1.1.61. National Drug Code (NDC) - An eleven-digit code assigned to each drug.

1.1.62. National Medicaid EDI HIPAA Workgroup (NMEH) – A CMS sponsored workgroup for state collaboration in response to the original HIPAA mandates.

1.1.63. National Provider Identifier (NPI) - A unique 10-digit identification number issued to health care providers in the United States by CMS.

1.1.64. National Uniform Billing Committee (NUBC) - A committee comprised of major national provider and payer organizations in order to develop a single billing form and standard data sets that could be used nationwide by institutional providers and payers for handling diagnosis codes within health care claims.

1.1.65. Open Source Software - Software that incorporates or has embedded in it any source, object or other software code subject to an "open source", "copyleft" or other similar type of license terms (including, without limitation, any GNU General Public License, Library General Public License, Lesser General Public License, Mozilla License, Berkeley Software Distribution License, Open Source Initiative License, MIT license, Apache license, and the like).

1.1.66. Operational Start Date – The date on which the Department authorizes Contractor to begin the PBMS Ongoing Operations and Enhancement Contract Stage.

1.1.67. Optical Character Recognition (OCR) - The mechanical or electronic conversion of scanned images of handwritten, typewritten or printed text into machine-encoded text for the purpose of electronically searching, storing more compactly, on-line display, and text mining.

1.1.68. Organizational Readiness – The readiness of the Contractor, as an entity, and the Department.

1.1.69. Operational Readiness – The readiness of the PBMS to function, and of the Contractor and the Department to operate the PBMS, in accordance with the requirements of this Contract.

1.1.70. Preferred Drug List (PDL) - A formal published list of specific Prescription drug products by brand and generic name that may be reimbursed without a PA.

1.1.71. Prescription - A written, faxed or oral order, as required by the Board of Pharmacy, from a practitioner that a certain drug, medical supply, device or service is medically necessary.

1.1.72. Prior Authorization (PA) - A requirement mandating that a provider must obtain approval to perform a service or prescribe a specific medication prior to performing the service or prescribing the medication, and is the record of the approved request.

1.1.73. Problem - A Defect, operational issue or situation regarded as unwelcome or harmful and needing to be dealt with and overcome.

1.1.74. Production Environment - The System hardware and software environment designated to the final stage in the release process, which serves the end-users.

1.1.75. Program Integrity (PI) – Activities completed by the Department or other entities concerning monitoring the utilization habits and patterns of both members and providers of the Colorado Medical Assistance Program to create a culture where there are consistent incentives to provide better health outcomes within a context that avoids over- or underutilization of services.

1.1.76. Protected Health Information (PHI) - Individually identifiable health information or health information with data items that reasonably could be expected to allow individual identification.

1.1.77. Provider – An individual or entity furnishing medical, mental health, dental or pharmacy services.

1.1.78. Provider Enrollment - A completed capture and verification of provider demographic, licensure, disclosure information, and an executed provider participation agreement, including a Provider Revalidation.

1.1.79. Provider Revalidation - A completed evaluation verifying that a provider meets Federal and State conditions for participation in accordance with the ACA Provider Screening Rule.

1.1.80. Quality Assurance (QA) - The planned and systematic activities implemented in a quality system so that quality requirements for a product or service will be fulfilled.

1.1.81. Requirements Traceability Matrix (RTM) - A document that compares any two baseline documents that require a many-to-many relationship to determine the completeness of the relationship.

1.1.82. Service Oriented Architecture (SOA) - Represents software architecture comprised of interoperable, discoverable, and potentially reusable services.

1.1.83. Single Sign-On (SSO) - An access control feature of Software applications that allows a user to log in once and gain access to all associated applications, without being prompted to log in for each.

1.1.84. Software - A set of programs, procedures, algorithms and its documentation concerned with the operation of a data processing system.

1.1.85. Specification - A detailed, exact statement of particulars such as a statement prescribing materials, dimensions and quality of work.

1.1.86. State Fiscal Year (SFY) - The period which begins on July 1 of each calendar year and ends on June 30 of the following calendar year.

1.1.87. State Self-Assessment (SS-A) - A structured method used to document a state's current Medicaid business enterprise by aligning a state's business areas to the MITA business areas and business processes.

1.1.88. Statement on Standards for Attestation Engagements No. 16 (SSAE-16) - The authoritative guidance for reporting on service organizations promulgated by the American Institute of Certified Public Accountants.

1.1.89. System – The collection of technical and/or automated functions within the PBMS.

1.1.90. Systems Development Life Cycle (SDLC) - A process of creating or altering information systems, and the models and methodologies that are used to develop these systems. The methodologies form the framework for planning and controlling the creation of an information system.

1.1.91. Technology Stack - A Technology Stack comprises the layers of components or services that are used to provide a software solution or application.

1.1.92. Third Party Liability (TPL) – The liability of an entity that is, or may be, liable to pay all or part of the medical cost of care for a Medicaid client.

1.1.93. Transaction Control Number (TCN) - The unique claim identifier used by the Legacy System.

1.1.94. Transmittal - An official document from the Department authorizing the Contractor to perform a specific function that is considered within the Contractor's Scope-of-Work during the Contract, but a Transmittal may not be used for any changes that require an SDLC or follow the Change Management Process.

1.1.95. UAT Environment – The System hardware and software environment designated for UAT, in which the Department may perform tests prior to the System or modifications to the System being made available in the Production Environment.

1.1.96. User Acceptance Testing (UAT) - The process to obtain confirmation that a system meets mutually agreed-upon requirements prior to the Department's acceptance of the System or changes to the System.

1.1.97. User Interface (UI) – The interface between the PBMS and users.

1.1.98. Web Portal - A secure Internet website that contains forms and other information specific to the system and provides the Medical Assistance program enterprise a consistent look and feel for the various applications.

EXHIBIT G, PERFORMANCE STANDARDS

In addition to the performance standards listed in Exhibit E for which the Contractor may earn a QMP, the Contractor shall also comply with all of the performance standards contained in the following table:

Non-QMP Performance Standards
Reference #2339: The Contractor shall report any unscheduled PBMS downtime within thirty (30) minutes of incident.
Reference #2363: PBMS User Guides/Help updates shall be completed within five (5) days of notification by the Department of the change.
Reference #2364: PBMS screen and functionality FAQ updates shall be completed within five (5) Business Days of notification by the Department of the change.
Reference #2469, #2470, #2471, #2472, #2473: Within forty-eight (48) hours Contractor shall resolve any enrollment issues within their control.
Reference #2558: The IVR shall be available 24 hours a day, 7 days a week, other than scheduled maintenance periods.
All voice and e-mail messages sent by the Department will receive a response within one (1) Business Day. A response does not mean resolution is provided; instead it may include a simple acknowledgement of the inquiry or referral to another representative as long as the representative responds within the same timeframe. If the response is a referral to another representative, the response shall provide a target completion or resolution date. The Contractor shall not be required to provide a regular report or measure metrics on this performance standard, but shall provide support that it has met this standard on a per-incident basis, upon request by the Department.
As agreed upon and approved by the Department, a performance survey will be provided to the Providers, and/or the Providers' designee, no more often than semi-annually. The results of this survey shall be satisfactory or better.

In the event that the Contractor fails to meet one of the Non-QMP Performance Standards described in this section, then the Contractor shall provide the Department with a corrective action plan on how they will correct or prevent the failure in the future.

EXHIBIT H, STATE CYBERSECURITY POLICIES

1. INCLUDED CYBERSECURITY POLICIES

1.1. This Exhibit contains the following State Cybersecurity Policies, attached hereto and incorporated herein:

1.1.1. P-CISP-001 – Access Control

1.1.2. P-CISP-002 – Security Awareness and Training

1.1.3. P-CISP-003 – Audit and Accountability

1.1.4. P-CISP-004 – Security Assessment and Authorization

1.1.5. P-CISP-005 – Configuration Management

1.1.6. P-CISP-006 – Contingency Planning

1.1.7. P-CISP-007 – Identification and Authentication

1.1.8. P-CISP-008 – Incident Response

1.1.9. P-CISP-009 – System Maintenance

1.1.10. P-CISP-010 – Media Protection

1.1.11. P-CISP-011 – Physical and Environmental Protection

1.1.12. P-CISP-012 – Personnel Security

1.1.13. P-CISP-013 – Risk Assessment

1.1.14. P-CISP-014 – System and Services Acquisition

1.1.15. P-CISP-015 – System and Communications Protection

1.1.16. P-CISP-016 – System and Information Integrity

1.1.17. P-CISP-017 – Security Planning

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-008 Access Control.

The purpose of this policy is to ensure that State of Colorado information systems have appropriate access control requirements implemented. Access to state information systems must be controlled to ensure only those users who are authorized may access these information systems. Approval for access is granted by the information system owner or their designee.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

5. REFERENCES

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. TERMS AND DEFINITIONS

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

6.1. **Access Controls**: Access controls are typically logical controls designed into the hardware and software of a computing system. Identification is accomplished both under program control and physical controls.
6.2. **CISO:** Chief Information Security Officer.
6.3. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.4. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.5. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.6. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.7. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies .

7. REQUIREMENTS:

7.1. Account Management (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall identify and select specific types of information system accounts to support organizational missions/business functions. Information account types include individual, shared, group, system, guest/anonymous, emergency, developer, manufacturer/vendor, temporary and service.

7.1.3. Agency shall establish conditions for group and role membership.

7.1.4. Agency shall specify and document authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

7.1.5. Agency shall require approvals by Workforce Supervisor for requests to create information system accounts.

7.1.6. Agency shall create, enable, modify, disable, and remove information system accounts in accordance with the Agency defined procedures, standards or requirements.

7.1.7. Agency shall monitor the use of information system accounts.

7.1.8. Agency shall notify access control team:

- When accounts are no longer required,
- When users are terminated or transferred, and/or
- When individual information system usage or need-to-know changes.

7.1.9. Agency shall authorize access to information systems based on:

- A valid access authorization, and
- Intended system usage.

7.1.10. Agency shall periodically review accounts for compliance (at least annually) with account management requirements.

7.1.11. Agency shall establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

7.1.12. Agency shall employ automated mechanisms to support the management of information system accounts.

7.1.13. The information system automatically disables inactive accounts after 90 days of inactivity.

7.2. Access Enforcement (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. The information system enforces approved authorizations for logical access to information and system resources.

7.3. Information Flow Enforcement (M)

7.3.1. This control is required for information systems with a **Moderate** security categorization.

7.3.2. The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems.

7.4. Separation of Duties (M)

7.4.1. This control is required for information systems with a **Moderate** security categorization.

7.4.2. Agency shall ensure, document, and enforce separation of duties.

7.5. Least Privilege (M)

7.5.1. This control is required for information systems with a **Moderate** security categorization.

7.5.2. Agency shall employ the principle of least privilege for all authorized accounts.

7.6. Unsuccessful Logon Attempts (LM)

7.6.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.6.2. Agency shall enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15 minute time period.

- Information systems containing FTI or HIPAA data shall enforce a limit of three (3) consecutive invalid logon attempts by a user during a 15 minute period.

7.6.3. Agency shall automatically perform a specified action, such as account lock, when the maximum number of unsuccessful attempts is exceeded.

7.7. System Use Notification (LM)

7.7.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.7.2. The information system shall be configured to display to users a system use notification banner before granting access to the system that provides privacy and security notices consistent with applicable laws.

7.7.3. The information system shall retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions (such as Click OK) to log on or further access the information system.

7.8. Previous Logon Notification

7.8.1. Where technically feasible, the information system shall notify the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

7.9. Session Lock (M)

7.9.1. This control is required for information systems with a **Moderate** security categorization.

7.9.2. The information system shall enforce automatic time out (prohibiting access to data) after 20 minutes of inactivity.

7.9.3. The information system retains the session lock until the user reestablishes access using established identification and authorization procedures.

7.10. Session Termination (M)

7.10.1. This control is required for information systems with a **Moderate** security categorization.

7.10.2. The information system automatically terminates a user session after a timeframe appropriate to the use of the information system and the needs of the agency.

- For information systems containing FTI data, this timeframe shall not exceed 15 minutes.

7.11. Remote Access (LM)

7.11.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.11.2. Agency shall establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

7.11.3. Agency shall implement appropriate internal controls based on system architecture and data classification.

7.11.4. Agency shall authorize remote access to the information system prior to allowing such connections.

7.12. Wireless Access (LM)

7.12.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.12.2. Agency shall establish and document usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

7.12.3. Agency shall authorize wireless access to the information system prior to allowing such connections.

7.12.4. Agency shall define appropriate controls for key management, usage and rotation.

7.13. Access Control for Mobile Devices (LM)

7.13.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.13.2. Agency shall establish and document usage restrictions, configuration/connection requirements, and implementation guidance for mobile devices.

7.13.3. Agency shall authorize the connection of mobile devices to organizational information systems.

7.13.4. Agency shall provide standards for State owned and personal mobile devices following industry best practices.

7.14. Use of External Information Systems (LM)

7.14.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.14.2. Agency shall establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
- Access the information system from external information systems; and
- Process, store or transmit organization-controlled information using external information systems.

7.14.3. Agency shall document procedures for accessing the information system from external information systems.

7.15. Information Sharing (M)

7.15.1. This control is required for information systems with a **Moderate** security categorization.

7.15.2. Agency shall establish procedures to enable authorized users to make information sharing/collaboration decisions.

7.16. Publicly Accessible Content (LM)

7.16.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.16.2. Agency shall designate individuals authorized to post information onto publicly accessible information systems.

7.16.3. Agency shall train authorized individuals to ensure publicly accessible information does not contain nonpublic information.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Information System Owner (or Designee)

8.2.1. Identify appropriate information system accounts, and approve access request forms.

8.3. Software Development Teams

8.3.1. Ensure access control requirements are developed for all agency applications.

8.4. Network Teams

8.4.1. Ensure remote access and wireless access requirements are met for each agency application.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-015 Security Training and Awareness.

The purpose of this policy is to ensure that State of Colorado personnel become aware of cyber security issues and their responsibilities to the data they protect by completing an annual Security Awareness Training.

- State personnel are required to read and be aware of policies, regulations, standards and guidance around protecting the State of Colorado information and information systems.
- Employees must complete security awareness training within the first 30 days of their employment, and annually thereafter.
- Additional training is required for those users who utilize sensitive data such as Federal Tax Information (FTI), Health Insurance Portability Accountability Act (HIPAA) data, and Payment Card Industry (PCI) data.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally

Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.4. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. Security Awareness Program (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall develop and document a security awareness and training program and disseminate the program to agency personnel.

7.1.3. Agency shall review and update the security awareness and training program annually.

7.2. Security Awareness Training (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. Agency shall provide basic security awareness training to information system users (including managers, senior executives and contractors):

- As part of initial training for new users,
- When required by information system changes, and
- Annually thereafter.

7.3. Role Based Security Training (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall provide role based security training to personnel with assigned security roles and responsibilities:

- Before authorizing access to the information system or performing assigned duties,
- When required by information system changes, and
- Annually thereafter.

7.4. Security Training Records (LM)

7.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.4.2. Agency shall document and monitor individual information system security training activities.

7.4.3. Agency shall retain individual training records for one (1) year or as required by applicable state and federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Human Resources Teams

8.2.1. Document and retain individual training records.

8.3. Agency Security or Training Team

8.3.1. Develop and deliver annual security training to agency personnel.

8.3.2. Develop and deliver role based security training curriculum for agency personnel with assigned security roles and responsibilities.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes portions of several policies: P-CISP-007 Systems and Applications Security Operations, P-CISP-008 Access Control and P-CISP-017 Security Metrics and Measurement Policy.

The purpose of this policy is to ensure information systems throughout the State of Colorado appropriately record auditable events as required by applicable state and federal laws, Executive Orders, directives, policies, regulations, standards and guidance. Auditable events are logged, stored, reviewed, and reported to ensure the information utilized by state employees is correct and is accessed only by authorized users.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy.

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.4. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.5. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.6. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies .

7. REQUIREMENTS:

7.1. Audit Events (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall identify events which are significant and relevant to the security and compliance of their information systems, and the environments in which the systems operate.

7.1.3. Auditable events shall include but not be limited to:

- Successful and failed logons
- Administrative privilege usage
- Attempted privilege escalation
- Change of file or user permissions or privileges
- Successful access from known malicious locations
- Brute force logon attempts users and sources list
- Intrusion attempt

7.2. Content of Audit Records (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. Information systems shall generate audit records containing information that shall include:

- Type of event occurred
- Date and time the event occurred
- Where the event occurred
- The source of the event
- The outcome of the event
- The identity of any individuals or subjects associated with the event

7.3. Audit Storage Capacity (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall allocate audit record storage capacity in accordance with the security requirements to handle security incidents and compliance mandates.

7.4. Response to Audit Processing Failures (LM)

7.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.4.2. Agency shall establish a procedure to prevent, detect, and respond to audit processing or audit system failures.

7.5. Audit Review, Analysis and Reporting (LM)

7.5.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.5.2. Agency shall review and analyze information system audit records for inappropriate or unusual activity quarterly or as required by applicable state or federal laws.

7.6. Audit Reduction and Report Generation (M)

7.6.1. This control is required for information systems with a **Moderate** security categorization.

7.6.2. Agency shall implement logging, monitoring, and reporting capabilities to ensure security and compliance.

7.7. Time Stamps (LM)

7.7.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.7.2. The information system shall be synchronized to the Department of Commerce (DOC) National Institute of Standards and Technology (NIST) Boulder Labs time source to ensure the integrity and correlation of the logs.

7.8. Protection of Audit Information (LM)

7.8.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.8.2. Agency shall protect audit information and audit tools from unauthorized access, modification and deletion.

7.9. Audit Record Retention (LM)

7.9.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.9.2. Agency shall retain audit records for one (1) year or as required by applicable state and federal laws to provide support for after-the-fact investigations of security incidents and to meet regulatory audit record retention requirements.

7.9.3. Agency shall retain audit records for seven (7) years for FTI information systems.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Security Operations Team

8.2.1. Define specific security auditable events for information systems.

8.2.2. Define required security audit processing failure actions.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may

result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-016 Self Assessment Policy.

The purpose of this policy is to ensure state information systems perform security assessments to measure adherence to established policies.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

6.1. **Authorizing Official**: A senior agency official who can make the decision to authorize operation of an information system, and to explicitly accept the risk to the agency operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations based on the implementation of an agreed-upon set of security controls.
6.2. **CISO**: Chief Information Security Officer.
6.3. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.4. **Critical Information System**:An application that provides critical services to the public and its operation serves a vital function to government, but does not impact life safety.
6.5. **Essential Information System**: An application which is so important to the agency that its loss or unavailability is unacceptable due to life safety issues.
6.6. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.7. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.8. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.9. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality,

integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies .

7. REQUIREMENTS:

7.1. Security Assessments (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall develop a security assessment plan that describes the scope of the assessment including:

- Security controls and control enhancements under assessment,
- Assessment procedures to be used to determine security control effectiveness, and
- Assessment environment, assessment team, and assessment roles and responsibilities.

7.1.3. Agency shall assess the security controls in the information system and its environment of operation annually or when a major change is implemented.

7.1.4. Agency shall produce a security assessment report that documents the results of the assessment and distribute the report to appropriate personnel.

7.2. System Interconnections (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. Agency shall authorize connections from the information system to other information systems through the use of Interconnection Security Agreements.

7.2.3. Agency shall document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.

7.2.4. Agency shall review and update Interconnection Security Agreements annually.

7.3. Plan of Action and Milestones (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall develop a plan of action and milestones (POAM) for the information system to document the organization's planned remedial actions.

7.3.3. Agency shall update existing POAMs quarterly based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

7.4. Security Authorization (LM)

7.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.4.2. Agency shall assign a senior-level executive or manager as the authorizing official for the information system.

7.4.3. Agency shall ensure that the authorizing official authorizes the information system for processing before commencing operations.

7.5. Continuous Monitoring (LM)

7.5.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.5.2. Agency shall develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

- Establishment of metrics to be monitored,
- Establishment of frequency for monitoring and for assessments supporting such monitoring,
- Ongoing security control assessments in accordance with the organizational continuous monitoring strategy,
- Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy,
- Correlation and analysis of security-related information generated by assessments and monitoring, and
- Response actions to address results of the analysis of security-related information.

7.6. Internal System Connections (LM)

7.6.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.6.2. Agency shall review and authorize internal connections between information systems.

7.6.3. Agency shall document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Information Security Officer

8.2.1. Perform agency information system audits.

8.2.2. Develop and monitor a POAM for audit security findings.

8.2.3. Submit Agency Cyber Security Plan (ACSP) to the state CISO annually on or before July 15.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-009 Change Control Policy.

The purpose of this policy is to ensure state assets adhere to secure configuration management. It also ensures changes to the security configuration are managed through change control so the changes are reviewed, tested, validated and documented. This policy also ensures each agency establishes software usage restrictions including license tracking and establishes a process for users to request non-standard software.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information SystemsFederal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.4. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.5. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **Authorizing Official**: A senior agency official who can make the decision to authorize operation of an information system, and to explicitly accept the risk to the agency operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations based on the implementation of an agreed-upon set of security controls.
6.2. **CISO**: Chief Information Security Officer.
6.3. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.4. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.5. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.6. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.7. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the

Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. Baseline Configuration (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall develop, document and maintain a current baseline configuration of information systems and system components (e.g., software packages, version numbers, and patch information).

7.1.3. Agency shall review and update the baseline configuration of the information system, annually or when changes occur that may have potential impact to security controls such as when system components are installed, changed, or upgraded.

7.1.4. Agency shall retain a previous version(s) of the baseline configuration to support rollback.

7.1.5. Agency shall ensure mobile devices connect to the state network monthly to receive configuration changes, anti-virus updates and patch updates.

7.2. Configuration Change Control (M)

7.2.1. This control is required for information systems with a **Moderate** security categorization.

7.2.2. Agency shall determine the types of changes to the information system that are configuration-controlled.

7.2.3. Agency shall review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analysis.

7.2.4. Agency shall test, validate, and document any changes to the information system before implementing the changes on the operating system.

7.2.5. Agency shall make approved changes to the system including modifications to hardware, software, or firmware components and configuration settings as defined in Configuration Settings (below).

7.2.6. Agency shall document configuration change decisions associated with the information system.

7.2.7. Agency shall retain records of configuration-controlled changes to the information system for one (1) year or as required by applicable state or federal laws.

7.2.8. Agency shall audit and review activities associated with configuration-controlled changes to the information system.

7.2.9. Agency shall coordinate and provide oversight for configuration change control activities through a Change Control Committee or Board.

7.3. Security Impact Analysis (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall analyze changes to the information system to determine potential security impacts, and the associated security ramifications (e.g., to security plan or risk assessment), prior to change implementation.

7.4. Access Restrictions for Change (M)

7.4.1. This control is required for information systems with a **Moderate** security categorization.

7.4.2. Agency shall ensure only authorized personnel are able to implement approved configuration changes.

7.5. Configuration Settings (LM)

7.5.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.5.2. Agency shall establish and document secure configuration settings for information technology products (e.g., mainframe computer, servers, workstations, and other network components) employed within the information system using the Center for Internet Security (CIS) standards.

7.5.3. Agency shall identify, document, and approve any deviations from established secure configuration settings.

7.5.4. Agency shall monitor and control changes to the secure configuration settings in accordance with organizational policies and procedures.

7.6. Least Functionality (LM)

7.6.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.6.2. Agency shall configure the information system to provide only essential capabilities.

7.6.3. Agency shall harden systems to include prohibiting, disabling, or restricting the use of unused or unnecessary physical and logical functions, ports, protocols and/or services.

7.6.4. Agency shall periodically review the information system to identify unnecessary and/or nonsecure functions, ports, protocols, and services and disable those deemed to be unnecessary and/or nonsecure.

7.6.5. Agency shall ensure the information system allows only authorized software program execution.

7.6.6. Agency shall review and update the list of authorized software that can be installed on the information system quarterly or as required by applicable state or federal laws.

7.7. Information System Component Inventory (LM)

7.7.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.7.2. Agency shall develop and document an inventory of information system components that accurately reflects the current information system.

7.7.3. Agency shall scan the network to detect changes to the asset inventory. Automated tools which provide continuous scanning abilities are preferable to a manual scan review. However, if the inventory scan to detect changes is manual, it must be reviewed quarterly.

7.7.4. Agency shall ensure unauthorized devices are removed from the network.

7.7.5. Agency shall review and update the asset inventory. Automated tools which provide continuous scanning abilities are preferable to a manual scan review. However, if the asset inventory scan is manual, it must be reviewed quarterly.

7.8. Configuration Management Plan (M)

7.8.1. This control is required for information systems with a **Moderate** security categorization.

7.8.2. Agency shall ensure a configuration management plan is developed, documented and implemented for the information system that:

- Addresses roles, responsibilities and configuration management processes and procedures.
- Establishes a process for identifying configuration items (i.e., hardware, software, firmware, and documentation) throughout the system development life cycle and for managing the configuration of the configuration items.
- Defines the configuration items for the information system and places the configuration items under configuration management.
- Protects the configuration management plan from unauthorized disclosure and modification.
- Describes how to: move changes through the change management processes, update configuration settings and baselines, maintain information system component inventories, control development, test, and operational environments, and develop, release, and update key system documentation.

7.9. Software Usage Restrictions (LM)

7.9.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.9.2. Agency shall use software and associated documentation in accordance with contract agreements and copyright laws.

7.9.3. Agency shall track the use of software and associated documentation protected by quantity licenses to control copying and distribution. Automated tracking tools which provide continuous scanning abilities are preferred. However, if the software usage tracking is performed manually, it must be reviewed quarterly.

7.9.4. Agency shall control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for unauthorized distribution, display, performance or reproduction of copyrighted work.

7.10. User Installed Software (LM)

7.10.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.10.2. Agency shall establish policies that govern the installation of software by users.

7.10.3. Agency shall enforce software installation policies through procedure, periodic examination, and/or automated methods. Automated inventory tools which provide continuous scanning abilities are preferred. However, if user software tracking is performed manually, it must be reviewed quarterly.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Information Security Officer

8.2.1. Establish security configuration settings for information technology products.

8.2.2. Perform information system component inventory scans as required.

8.2.3. Create and implement a configuration management plan.

8.2.4. Track licensing of agency software.

8.2.5. Create a list of acceptable software for the agency.

8.2.6. Ensure software audits are performed regularly.

8.2.7. Implement a software request and approval process for agency personnel.

8.3. Agency Network and Server Teams

8.3.1. Create and maintain baseline configuration management documentation.

8.3.2. Participate in Change Management activities.

8.3.3. Create and maintain an information system component inventory.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-004 Disaster Recovery Policy.

The purpose of this policy is to ensure agency information systems that are determined to be critical and essential to the agency mission have recovery objectives defined, documented and tested in the case of a catastrophic failure of the information systems.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information SystemsFederal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.4. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.5. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy.

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Critical Information System**:An application that provides critical services to the public and its operation serves a vital function to government, but does not impact life safety.
6.4. **Essential Information System**: An application which is so important to the agency that its loss or unavailability is unacceptable due to life safety issues.
6.5. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.6. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.7. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.8. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. Contingency Plan (LM, Critical or Essential [or equivalent] Only)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization that are also classified as a **Critical** or **Essential** (or equivalent) information system.

7.1.2. Agency shall create a Contingency Plan which:

- Identifies essential missions and business functions and associated contingency requirements,
- Provides recovery objectives, restoration priorities and metrics,
- Addresses contingency roles, responsibilities, and assigned individuals with contact information,
- Plans for the resumption of essential missions and business functions,
- Identifies critical technical and operational assets that support essential missions and functions,
- Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented, and
- Is reviewed and approved by key business and information system leaders or their designees.

7.1.3. Agency shall distribute copies of the contingency plan to key business and information system leaders or their designees.

7.1.4. Agency shall coordinate contingency planning activities with incident handling activities and other plans such as business continuity plans, continuity of operation plans, and security incident response plans.

7.1.5. Agency shall review and update the contingency plan for the information system(s) annually or when changes are made to the information system(s).

7.1.6. Agency shall communicate contingency plan changes to key business and information system leaders or their designees.

7.1.7. Agency shall protect the contingency plan from unauthorized disclosure, inspection, and modification.

7.2. Contingency Training (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. Agency shall provide contingency plan training to personnel with assigned security roles and responsibilities:

- Prior to being assigned a contingency role or responsibility,
- When required by information system changes, and
- Annually thereafter.

7.3. Contingency Plan Testing (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall test the contingency plan for the information system annually.

7.3.3. Agency shall coordinate testing of the contingency plan with organizational elements responsible for related plans such as business continuity, continuity of operations, and security incident response plans.

7.3.4. Agency shall review the contingency plan test results within 30 calendar days, and communicate the results to key business and information system leaders or their designees.

7.3.5. Agency shall initiate and document corrective actions, if needed.

7.4. Alternate Storage Site (M)

7.4.1. This control is required for information systems with a **Moderate** security categorization.

7.4.2. Agency shall establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.

- Agency shall ensure agreements define circumstances such as environmental conditions, site access rules, physical and environmental protection needs, and coordination of delivery and retrieval of backup media.
- Agency shall ensure alternate storage site operating conditions complement business continuity plans to permit maintenance of essential functions despite availability of an information system.
- Agency shall designate an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

7.4.3. Agency shall ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

7.5. Alternate Processing Site (M)

7.5.1. This control is required for information systems with a **Moderate** security categorization.

7.5.2. Agency shall establish an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations.

7.5.3. Agency shall ensure the agreement contains priority-of-service provisions in accordance with Agency requirements such as recovery time objectives.

7.5.4. Agency shall ensure that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the recovery time objective requirements.

7.5.5. Agency shall ensure the alternate processing site provides information security safeguards equivalent to that of the primary site.

7.6. Telecommunications Services (M)

7.6.1. This control is required for information systems with a **Moderate** security categorization.

7.6.2. Agency shall determine requirements to establish alternate telecommunications services including necessary agreements to permit the resumption of information system operations necessary for essential missions and business functions.

7.6.3. Agency shall determine requirements to obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

7.6.4. Agency shall ensure alternate telecommunications services agreement provisions consider availability, quality of service, access, and priority-of-service in accordance with the Agency's information system availability requirements.

7.7. Information System Backup (LM)

7.7.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.7.2. Agency shall conduct backups of user and system-level information contained in the information system as required to support the business function.

7.7.3. Agency shall conduct backups of information system documentation including security-related documentation as required to support the business function.

7.7.4. Agency shall monitor backups to ensure successful completion and take corrective action if the backup did not complete successfully.

7.7.5. Agency shall protect the confidentiality, integrity, and availability of backup information at primary and alternate storage locations.

7.7.6. Agency shall test backup information in accordance with Agency requirements such as recovery time objectives, to verify media reliability and information integrity.

7.8. Information System Recovery and Reconstitution (LM)

7.8.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.8.2. Agency shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise or failure.

7.8.3. The information system shall implement transaction recovery (e.g., transaction rollback and transaction journaling) for systems that are transaction-based; for example, database management systems and transaction processing systems.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Information Security Officer

8.2.1. Ensure disaster recovery plans are in place for agency-defined critical and essential applications.
8.2.2. Ensure agency disaster recovery plans are tested annually and results are communicated to participants.
8.2.3. Ensure agency disaster recovery plans are reviewed and updated at least annually, or when changes to the information systems require an update.
8.2.4. Assist agency Network and Server teams in testing backup media to verify information integrity.

8.3. Agency Network and Server Teams

8.3.1. Ensure required information system backups are performed.
8.3.2. Test backup media quarterly to verify media reliability and information integrity.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-008 Access Control Policy.

The purpose of this policy is to ensure each individual or system is assigned a unique identifier (user/system ID) and authenticator (password) for agency information system access.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **Agency User**: An agency employee or an individual the agency deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship.
6.2. **CISO**: Chief Information Security Officer.
6.3. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.4. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.5. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.6. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.7. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. Identification and Authentication [Agency Users] (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. The information system shall uniquely identify and authenticate agency users and devices (or processes acting on behalf of agency users).

7.1.3. Agency shall implement multifactor authentication for remote access to the Agency resources for data classified with a Security Category of moderate or high.

7.1.4. Agency shall implement multifactor authentication for local access to system administrative accounts for critical systems.

7.2. Device Identification and Authentication (M)

7.2.1. This control is required for information systems with a **Moderate** security categorization.

7.2.2. The information system shall uniquely identify and authenticate devices before establishing a remote network connection.

7.3. Identifier Management (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall obtain authorization from appropriate information system owners to assign or create an individual, group, role or device identifier or account.

7.3.3. Agency shall select an identifier that uniquely identifies an individual, group, role, or device.

7.3.4. Agency shall assign the identifier to the intended individual, group, role, or device.

7.3.5. Agency shall archive inactive or terminated user credentials.

7.3.6. Agency shall develop a process for validating system users who request reinstatement of user credentials for those suspended or revoked by the system.

7.3.7. Agency shall prevent reuse of identifiers.

7.3.8. Agency shall disable the identifier or account after employee transfer, termination, or other circumstances.

7.4. Authenticator Management (LM)

7.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.4.2. Agency shall verify, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

7.4.3. Agency shall establish initial authenticator content for authenticators defined by the organization.

7.4.4. Agency shall ensure that authenticators have sufficient strength of mechanism for their intended use and include the following.

- Minimum password complexity that includes at least nine (9) characters, mix of upper and lower-case letters, numbers and/or special characters.
- Prohibit password reuse for six (6) generations.

7.4.5. Agency shall establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

7.4.6. Agency shall change default content of authenticators prior to information system installation.

7.4.7. Agency shall establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.

7.4.8. Agency shall change/refresh authenticators per a pre-determined time period, based on type of authenticator.

7.4.9. Agency shall protect authenticator content from unauthorized disclosure and modification.

7.4.10. Agency shall require individuals to follow, and have devices implement specific security safeguards to protect authenticators.

7.4.11. Agency shall change authenticators for group/role accounts when membership to those accounts changes.

7.4.12. Agency shall store and transmit only encrypted representations of passwords.

7.5. Authenticator Feedback (LM)

7.5.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.5.2. The information system must obscure feedback of authentication information during the authentication (logon) process to protect the information from possible exploitation/use by unauthorized individuals.

7.6. Re-authentication (M)

7.6.1. This control is required for information systems with a **Moderate** security categorization.

7.6.2. As determined by the Agency, the information system requires users and devices to re-authenticate in situations:

- when authenticators change;
- when roles change;
- when security categories of information systems change;
- when the execution of privileged functions occurs; and/or
- after 20 minutes of inactivity.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Information System Owner

8.2.1. Identify appropriate system access, and approve access request forms.

8.3. Agency Information System Access Control Team

8.3.1. Assign unique identifiers to information system users, groups, roles or devices.

8.3.2. Follow information system requirements for authenticator management.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This Policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-002 Incident Response Plan.

The purpose of this policy is to ensure agencies have an incident response plan in place and that it is tested regularly. The incident response plan must include reporting requirements from applicable state and federal laws, Executive Orders, directives, policies, regulations, standards and guidance. These requirements are dependent upon the Security Category of the information utilized by agency information systems.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information SystemsFederal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.4. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.5. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.4. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.5. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.6. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. Incident Response Training (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall provide incident response training to personnel with assigned security roles and responsibilities:

- Prior to being assigned an incident response role or responsibility,
- When required by information system changes, and
- Annually thereafter.

7.2. Incident Handling (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. Agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

7.2.3. Agency shall coordinate incident handling activities with contingency planning activities.

7.2.4. Agency shall incorporate lessons learned from ongoing incident handling activities into incident response procedures, training and testing/exercises, and implements the resulting changes accordingly.

7.2.5. Agency shall employ a security incident management system designed to support the incident handling process.

7.3. Incident Monitoring (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall track and document information system security incidents and share this information with the appropriate stakeholders.

7.4. Incident Reporting (LM)

7.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.4.2. Agency shall require personnel to report suspected security incidents to the agency incident response capability no later than within 24 hours of discovering the incident.

7.4.3. Agency shall report security incidents according to the Agency incident response plan and/or Communications Plan.

7.4.4. Agency shall make timely report of security incidents to other state and federal agencies as required, based on the Security Category of the information system.

7.4.5. Agency shall implement automated mechanisms (e.g., online incident reporting or notification) to assist users in the reporting of security incidents.

7.5. Incident Response Assistance (LM)

7.5.1. This control is required for information systems with a **Low** or **Moderate** security categorization.
7.5.2. Agency shall provide an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.
7.5.3. Agency shall offer users automated mechanisms (e.g., website or proactive user messaging) to increase understanding and obtain incident response assistance and support.

7.6. Incident Response Plan (LM)

7.6.1. This control is required for information systems with a **Low** or **Moderate** security categorization.
7.6.2. Incident Response Plan shall provide the agency with a roadmap to handle security incidents.
7.6.3. Incident Response Plan shall describe the structure and agency of the incident response capability.
7.6.4. Incident Response Plan shall document the incident response team roles and responsibilities.
7.6.5. Incident Response Plan shall provide a high-level approach for how the incident response capability fits into the overall agency.
7.6.6. Incident Response Plan shall meet the unique requirements of the agency, which relate to mission, size, structure, and functions.
7.6.7. Incident Response Plan shall define reportable incidents.
7.6.8. Incident Response Plan shall provide metrics for measuring the incident response capability within the agency.
7.6.9. Incident Response Plan shall define the resources and management support needed to effectively maintain and mature an incident response capability.
7.6.10. Agency shall ensure key incident response team members have access to the incident response plan and procedures.
7.6.11. Agency shall review and approve the incident response plan at least annually or whenever changes to the information system have the potential to impact security controls.
7.6.12. Agency shall update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
7.6.13. Agency shall communicate incident response plan changes to key incident response personnel including data and system owners.
7.6.14. Agency shall protect the incident response plan from unauthorized disclosure and modification.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Incident Response Team

8.2.1. Follows the Agency Incident Response Plan and ensures requirements are defined and met for each incident.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CCSP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy does not supercede any previous policies.

The purpose of this policy is to ensure agencies have a plan for information system component maintenance. This helps to ensure that critical and essential business information system components are properly maintained and available for business functions.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information SystemsFederal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.4. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.5. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.4. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.5. **Media**: Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
6.6. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.7. **Sanitization**: Actions taken to render information stored on equipment or written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. The process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
6.8. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational

operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. Controlled Maintenance (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall schedule, perform, document and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or agency requirements.

7.1.3. Agency shall approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

7.1.4. Agency shall require that the information system owner explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

7.1.5. Agency shall sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.

7.1.6. Agency shall check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

7.1.7. Agency shall include maintenance-related information required by applicable state and federal laws, Executive Orders, directives, policies, regulations, standards and guidance in organizational maintenance records.

7.2. Maintenance Tools (M)

7.2.1. This control is required for information systems with a **Moderate** security categorization.

7.2.2. Agency shall approve, control, and monitor the use of, and maintain on an ongoing basis information system maintenance tools.

7.3. Non-Local (Remote) Maintenance (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall approve and monitor non-local maintenance and diagnostic activities.

7.3.3. Agency shall allow the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system.

7.3.4. Agency shall employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.

7.3.5. Agency shall maintain records for non-local maintenance and diagnostic activities.

7.3.6. Agency shall terminate session and network connections when non-local maintenance is completed.

7.4. Maintenance Personnel (LM)

7.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.4.2. Agency shall establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.

7.4.3. Agency shall ensure that non-escorted personnel performing maintenance on the information system have required access authorizations.

7.4.4. Agency shall designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

7.5. Timely Maintenance (M)

7.5.1. This control is required for information systems with a **Moderate** security categorization.

7.5.2. Agency shall obtain maintenance support and/or spare parts for information system components within the information system's required recovery time objective.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Server, Network and Desk Side Support Teams

8.2.1. Ensures maintenance requirements are documented for their respective areas of responsibility.

8.2.2. Ensures lists of approved maintenance personnel are up to date.

8.2.3. Monitors and escorts maintenance personnel as required.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes portions of P-CISP-011 Data Handling and Disposal.

The purpose of this policy is to ensure information system media is properly secured, stored, labeled and disposed of. The level of security required for information system media is dependent on the security category of the information residing on the information system.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies –http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information SystemsFederal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.4. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.5. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.4. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.5. **Media**: Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. For example, digital media includes diskettes, magnetic tapes, external/removable hard disk drives, flash drives, etc. Non-digital media includes paper and microfilm.
6.6. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.7. **Sanitization**: Actions taken to render information written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. The process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

6.8. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. Media Access (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall restrict access to digital and non-digital media to authorized users.

7.2. Media Marking (M)

7.2.1. This control is required for information systems with a **Moderate** security categorization.

7.2.2. Agency shall mark removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

7.3. Media Storage (M)

7.3.1. This control is required for information systems with a **Moderate** security categorization.

7.3.2. Agency shall physically control and securely store digital and non-digital media within a secure area.

7.3.3. Agency shall protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

7.4. Media Transport (M)

7.4.1. This control is required for information systems with a **Moderate** security categorization.

7.4.2. Agency shall protect and control digital and non-digital media during transport outside of controlled areas.

7.4.3. Agency shall maintain accountability for information system media during transport outside of controlled areas.

7.4.4. Agency shall document activities associated with the transport of information system media.

7.4.5. Agency shall restrict the activities associated with the transport of information system media to authorized personnel.

7.5. Media Sanitization (LM)

7.5.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.5.2. Agency shall sanitize digital and non-digital media prior to disposal, release out of organizational control, or release for reuse using required sanitization

techniques and procedures in accordance with NIST Special Publication 800-88 Rev1, Appendix A Minimum Sanitization Recommendations or applicable state, federal and agency standards and policies. Sanitization requirements are based on the security category of the information residing on the information system. Digital and non-digital media containing Federal Tax Information (FTI) must follow sanitization requirements detailed in the IRS Pub 1075.

7.5.3. Agency shall employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

7.6. Media Use (LM)

7.6.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.6.2. Agency shall ensure the use of only authorized removable information system media on information systems or system components using appropriate security safeguards.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-010 Physical Security Policy.

The purpose of this policy is to ensure information systems are effectively protected from physical threats including unauthorized access and environmental issues. The level of protection depends on the security category of the information residing on the information system.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies - http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.4. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.5. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.6. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. Physical Access Authorizations (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall develop, approve and maintain a list of individuals with authorized access to the facility where the information system resides.

7.1.3. Agency shall ensure that authorization credentials for facility access are properly issued by the overseeing agency.

7.1.4. Agency shall review the access list detailing authorized facility access by individuals quarterly.

7.1.5. Agency shall ensure that individuals are removed from the facility list when access is no longer required by the overseeing Agency.

7.2. Physical Access Control (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. Agency shall ensure the physical access authorizations at entry/exit points to the facility where the information system resides is enforced by the overseeing agency by validating the following:

- Verifying individual access authorizations before granting access to the facility; and
- Controlling ingress/egress to the facility using physical access control systems/devices or guards.

7.2.3. Agency shall maintain physical access audit logs for entry and exit points.

7.2.4. Agency shall provide security safeguards commensurate with applicable state and federal laws, Executive Orders, directives, policies, regulations, standards and guidance as defined by the information system data security categorization to control access to areas within facilities officially designated as publicly accessible.

7.2.5. Agency shall escort visitors and monitor visitor activity in all secure areas.

7.2.6. Agency shall secure keys, combinations, and other physical access devices.

7.2.7. Agency shall inventory physical access devices annually.

7.2.8. Agency shall change combinations and keys annually and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

7.3. Access Control for Transmission Medium (M)

7.3.1. This control is required for information systems with a **Moderate** security categorization.

7.3.2. Agency shall control physical access to information system distribution and transmission lines within organizational facilities using required security safeguards.

7.4. Access Control for Output Devices (M)

7.4.1. This control is required for information systems with a **Moderate** security categorization.

7.4.2. Agency shall control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

7.5. Monitoring Physical Access (LM)

7.5.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.5.2. Agency shall ensure that monitoring of physical access to the facility where the information system resides is in place to detect and respond to physical security incidents.

7.5.3. Agency shall ensure a review of physical access logs is conducted annually and upon occurrence of a physical security violation.

7.5.4. Agency shall coordinate results of review and investigations with the organizational incident response capability.

7.6. Visitor Access Records (LM)

7.6.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.6.2. Agency shall ensure that visitor access records are maintained to the facility where the information system resides to meet applicable state and federal laws, Executive Orders, directives, policies, regulations, standards and guidance as defined by the information system data security categorization.

7.6.3. Agency shall ensure a review of visitor access records is conducted quarterly by the responsible agency.

7.7. Power Equipment and Cabling (M)

7.7.1. This control is required for information systems with a **Moderate** security categorization.

7.7.2. Agency shall ensure that proper protection of power equipment and power cabling for the information system from damage and destruction is being provided by the responsible agency.

7.8. Emergency Shutoff (M)

7.8.1. This control is required for information systems with a **Moderate** security categorization.

7.8.2. Agency shall ensure that the capability of shutting off power to the information system or individual system components in emergency situations is in place.

7.8.3. Agency shall ensure that emergency shutoff switches or devices to facilitate safe and easy access for personnel are provided by the responsible agency.

7.8.4. Agency shall ensure that protection to emergency shutoff capability from unauthorized activation is in place and properly maintained by the responsible agency.

7.9. Emergency Power (M)

7.9.1. This control is required for information systems with a **Moderate** security categorization.

7.9.2. Agency shall ensure that a short-term uninterruptible power supply is provided by the responsible agency to facilitate an orderly shutdown of the information

system, or transition of the information system to long-term alternate power in the event of a primary power source loss.

7.10. Emergency Lighting (LM)

7.10.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.10.2. Agency shall employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

7.11. Fire Protection (LM)

7.11.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.11.2. Agency shall employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

7.12. Temperature and Humidity Controls (LM)

7.12.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.12.2. Agency shall maintain appropriate temperature and humidity levels within the facility where the information system resides.

7.12.3. Agencies shall monitor temperature and humidity levels.

7.13. Water Damage Protection (LM)

7.13.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.13.2. Agency shall protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

7.14. Delivery and Removal (LM)

7.14.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.14.2. Agency shall authorize, monitor and control information system components entering and exiting the facility and maintains records of those items.

7.15. Alternate Work Site (M)

7.15.1. This control is required for information systems with a **Moderate** security categorization.

7.15.2. Agency shall employ appropriate security controls at alternate work sites.

7.15.3. Agency shall assess, as feasible, the effectiveness of security controls at alternate work sites.

7.15.4. Agency shall provide a means for employees to communicate with information security personnel in case of security incidents or problems.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-012 Personnel Security Policy.

The purpose of this policy is to help alleviate security risks brought on by agency personnel. It ensures agency personnel fulfill the screening criteria set up each agency and also ensures third-party personnel follow the same security criteria.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy.

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.4. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.5. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.6. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. Position Risk Designation (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall establish screening criteria for individuals filling agency roles according to position risk.

7.1.3. Agency shall review and update position risk designations annually or as necessary for the position.

7.2. Personnel Screening (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. Agency shall screen individuals prior to authorizing access to the information system.

7.2.3. Agency shall rescreen individuals every five (5) years or as necessary for the positions risk rating.

7.3. Personnel Termination (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Upon termination of individual employment:

- Agency Human Resources team notifies access control team to modify or terminate access.
- Agency shall disable information system access immediately.
- Agency shall conduct exit interviews that include a discussion surrendering resources and access information.
- Agency shall retrieve all security-related information system-related property.
- Agency shall retain access to information and information systems formerly controlled by terminated individual.

7.4. Personnel Transfer (LM)

7.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.4.2. Agency shall review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the Colorado State Government.

7.5. Access Agreements (LM)

7.5.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.5.2. Agency shall develop and document access agreements/Acceptable Use Policies for information systems.

7.5.3. Agency shall ensure individuals requiring access to information and information systems sign appropriate access agreements/Acceptable Use Policies prior to being granted access.

7.5.4. Agency shall review and update the access agreements/Acceptable Use Policies annually or as necessary for the position.

7.6. Third Party Personnel Security (LM)

7.6.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.6.2. Agency shall establish personnel security requirements including security roles and responsibilities for third-party providers.

7.6.3. Agency shall require third-party providers to comply with personnel security policies and procedures established by the agency.

7.6.4. Agency shall require third-party providers to comply with the personnel policy requirement as applicable.

7.7. Personnel Sanctions (LM)

7.7.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.7.2. Agency shall employ a formal sanctions process for individuals failing to comply with established information security policies and procedures.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Human Resources Teams

8.2.1. Ensures policy requirements are met, including termination and transfer notifications to system information owners and other appropriate personnel or teams.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-003 Information Risk Management Policy.

The purpose of this policy is to ensure agency information is appropriately categorized. It also ensures agencies perform risk assessments on the information systems which store the information and ensures vulnerability scans are performed on the information systems.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies -http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Critical Information System**: An application that provides critical services to the public and its operation serves a vital function to government, but does not impact life safety.
6.4. **Essential Information System**: An application which is so important to the agency that its loss or unavailability is unacceptable due to life safety issues
6.5. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.6. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.7. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.8. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.
6.9. **System Development Life Cycle (SDLC):** A process for planning, creating, testing and deploying an information system. This includes software and hardware components of an information system.

7. REQUIREMENTS:

7.1. Security Categorization (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall categorize information and the information system in accordance with applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

7.1.3. Agency shall document the security categorization results (including supporting rationale) in the security plan for the information system.

7.1.4. Agency shall ensure that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

7.1.5. Agency shall make the security categorization decision in conjunction with the state Chief Information Security Officer (CISO) or designee, the information system owner, and business owner.

7.2. Risk Assessment (LM, Critical or Essential [or equivalent] Only)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization that are also classified as a **Critical** or **Essential** (or equivalent) information system.

7.2.2. Agency shall conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

- The assessment of risk should evaluate threats from external parties such as service contractors, contractors operating information systems on behalf of the agency, individuals accessing agency information systems, and outsourcing entities.
- Risk assessment can be performed at all three tiers in the risk management hierarchy – the organizational level, the mission or business process level, or the information system level – and at any phase in the system development life cycle.

7.2.3. Agency shall document risk assessment results in a risk assessment report, a security compliance report, or in some other format.

7.2.4. Agency shall review risk assessment results within 30 calendar days upon completion of the risk assessment.

7.2.5. Agency shall disseminate risk assessment results to data and system owners and others who have a role and responsibility in information system risk assessments.

7.2.6. Agency shall update the risk assessment annually, upon request, and/or whenever there are significant changes to the information system or environment of operation including the identification of new threats and vulnerabilities.

7.3. Vulnerability Scanning (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall perform ongoing vulnerability scans on the information system and hosted applications.

7.3.3. Agency shall employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automated parts of the vulnerability management process by using standards for:
- Enumerating platforms, software flaws, and improper configurations;
- Formatting checklists and test procedures; and
- Measuring vulnerability impact.

7.3.4. Agency shall employ scanning tools that are capable of readily updating vulnerabilities as new ones are discovered, announced, and/or new scanning methods are developed.

7.3.5. Agency shall analyze vulnerability scan reports and results from security control assessments.

7.3.6. Agency shall remediate legitimate vulnerabilities in a timely manner as indicated in the remediation or corrective action plan in accordance with an organizational assessment of risk.

7.3.7. Agency is encouraged to share information obtained from the vulnerability scanning process and security control assessment with the state CISO (or designee) and others that have a role and responsibility in information system risk assessments to help eliminate similar vulnerabilities in other information systems (e.g., systemic weaknesses or deficiencies).

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Information System Owners

8.2.1. Categorizes data to appropriate security levels.

8.2.2. Assists OIT personnel in performing risk assessments as needed.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-005 Vendor Management Policy.

The purpose of this policy is to ensure vendors follow the same security requirements to which the state is subject and security documentation for information systems is completed and periodically reviewed and updated. It also ensures software is developed with security requirements embedded. These requirements are applicable to both state and vendor software developers.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies –http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy.

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies .

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.4. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.5. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.6. **Secure System Development Life Cycle (SSDLC):** A secure process for planning, creating, testing and deploying an information system. This includes software and hardware components of an information system.
6.7. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies .

7. REQUIREMENTS:

7.1. Allocation of Resources (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall determine information security requirements for the information system or information system service in mission/business process planning.

7.1.3. Agency shall determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process.

7.1.4. Agency shall establish a discrete line item for information security in organizational programming and budgeting documentation.

7.2. System Development Life Cycle (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. Agency shall manage the information system using a secure system development life cycle (SSDLC).

7.2.3. Agency shall define and document information security roles and responsibilities throughout the system development life cycle.

7.2.4. Agency shall identify individuals having information security roles and responsibilities.

7.2.5. Agency shall integrate the organizational information security risk management process into system development life cycle activities.

7.3. Acquisition Process (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with the security categorization of the information to be stored and organizational mission/business needs:

- Security functional requirements;
- Security assurance requirements;
- Security-related documentation requirements;
- Requirements for protecting security-related documentation;
- Description of the information system development environment and environment in which the system is intended to operate; and
- Acceptance criteria.

7.4. Information System Documentation (LM)

7.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.4.2. Agency shall obtain administrator documentation for the information system, system component, or information system service that describes:

- Secure configuration, installation, and operation of the system, component, or service;
- Effective use and maintenance of security functions/mechanisms; and
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

7.4.3. Agency shall obtain user documentation for the information system, system component, or information system service that describes:

- User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
- Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
- User responsibilities in maintaining the security of the system, component, or service.

7.4.4. Agency shall document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.

7.4.5. Agency shall protect the documentation as required, in accordance with the risk management strategy, and based on the security categorization of the information.

7.4.6. Agency shall distribute documentation to authorized requesters.

7.5. Security Engineering Principles (M)

7.5.1. This control is required for information systems with a **Moderate** security categorization.

7.5.2. Agency or selected vendor shall apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

7.6. External Information System Services (LM)

7.6.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.6.2. Agency shall require that providers of external information system services comply with organizational information security requirements in accordance with applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

7.6.3. Agency shall define and document government oversight and user roles and responsibilities with regard to external information system services.

7.6.4. Agency shall monitor security control compliance by external service providers on an ongoing basis.

7.7. Developer Configuration Management (M)

7.7.1. This control is required for information systems with a **Moderate** security categorization.

7.7.2. Agency shall require the developer of the information system, system component, or information system service to:

- Perform configuration management during system, component, or service design, development, implementation and operation;
- Document, manage, and control the integrity of changes to configuration items under configuration management;
- Implement only agency-approved changes to the system, component, or service;
- Document approved changes to the system, component, or service and the potential security impacts of such changes; and
- Track security flaws and flaw resolution within the system, component, or service.

7.8. Developer Security Testing and Evaluation (M)

7.8.1. This control is required for information systems with a **Moderate** security categorization.

7.8.2. Agency shall require the developer of the information system, system component, or information system service to:

- Create and implement a security assessment plan;
- Perform unit, integration, system, and regression testing/evaluation;
- Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
- Implement a verifiable flaw remediation process; and
- Correct flaws identified during security testing/evaluation.

7.9. Development Process, Standards and Tools (LM)

7.9.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.9.2. Agency shall require the developer of the information system, system component, or information system service to follow a documented development process that:

- Explicitly addresses security requirements;
- Identifies the standards and tools used in the development process;
- Documents the specific tool options and tool configurations used in the development process; and
- Documents, manages and ensures the integrity of changes to the process and/or tools used in development.

7.9.3. Agency shall review the development process, standards, tools, and tool options/configurations annually.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Software Development Teams

8.2.1. Ensures secure software coding requirements and best practices are followed.

8.2.2. Ensures configuration management requirements are met for each project.

8.2.3. Requests security testing and evaluation to be performed prior to information system implementation.

8.3. Agency Vendor Management Team

8.3.1. Ensures appropriate security requirements are included in Requests for Proposals (RFPs)

8.3.2. Ensures appropriate security requirements are included in contracts with vendors.

8.4. Agency Security Team

8.4.1. Ensures pre-implementation security scans are performed on all software development projects.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes portions of P-CISP-006 Network Operations, P-CISP-007 System and Applications Operations, P-CISP-018 Mobile Computing Policies.

The purpose of this policy is to ensure agency information systems and communications are protected against security threats, both external and internal. It ensures information is protected in transit and at rest, commensurate with the security category of the information.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy.

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.4. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.5. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.6. **Secure System Development Life Cycle (SSDLC):** A secure process for planning, creating, testing and deploying an information system. This includes software and hardware components of an information system.
6.7. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies .

7. REQUIREMENTS:

7.1. Application Partitioning (M)

7.1.1. This control is required for information systems with a **Moderate** security categorization.

7.1.2. The information system provides security segmentation that isolates user functions from system management functions.

7.2. Security Function Isolation (M)

7.2.1. This control is required for information systems with a **Moderate** security categorization.

7.2.2. The information system isolates security functions from nonsecurity functions.

7.3. Information in Shared Resources (M)

7.3.1. This control is required for information systems with a **Moderate** security categorization.

7.3.2. The information system prevents unauthorized and unintended information transfer via shared system resources. Information system will follow federal and state requirements for protecting information on shared system resources.

7.4. Denial of Service Protection (LM)

7.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.4.2. The information system protects against or limits the effects of denial of service attacks.

7.5. Boundary Protection (LM)

7.5.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.5.2. The information system:

- Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
- Implements subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and
- Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

7.6. Transmission Confidentiality and Integrity (M)

7.6.1. This control is required for information systems with a **Moderate** security categorization.

7.6.2. The information system protects the confidentiality and integrity of transmitted information.

7.7. Network Disconnect (M)

7.7.1. This control is required for information systems with a **Moderate** security categorization.

7.7.2. The information system terminates the network connection associated with a communications session at the end of the session or after 20 minutes of inactivity according to system functionality and sensitivity needs.

7.8. Cryptographic Key Establishment and Management (LM)

7.8.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.8.2. Agency shall establish and manage cryptographic keys for required cryptography employed within the information system in accordance with applicable state, local, and federal regulatory standards for key generation, distribution, storage, access, and destruction.

7.9. Cryptographic Protection (LM)

7.9.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.9.2. The information system implements required cryptographic uses and type of cryptography required for each use in accordance with information system sensitivity and applicable state and federal laws, Executive Orders, directives, policies, regulations, and standards.

7.10. Collaborative Computing Devices (LM)

7.10.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.10.2. The information system:

- Prohibits remote activation of collaborative computing devices unless specifically approved for a business need; and
- Provides an explicit indication of use to users physically present at the devices.

7.11. Public Key Infrastructure Certificates (M)

7.11.1. This control is required for information systems with a **Moderate** security categorization.

7.11.2. Agency shall issue public key certificates under an agency-defined certificate policy, or obtain public key certificates from an approved service provider.

7.12. Mobile Code (M)

7.12.1. This control is required for information systems with a **Moderate** security categorization.

7.12.2. Agency shall:

- Define acceptable and unacceptable mobile code and mobile code technologies;
- Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
- Authorize, monitor, and control the use of mobile code within the information system.

7.13. Voice Over Internet Protocol (M)

7.13.1. This control is required for information systems with a **Moderate** security categorization.

7.13.2. Agency shall:

- Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
- Authorize, monitor, and control the use of VoIP within the information system.

7.14. Secure Name/Address Resolution Service (Authoritative Source) (LM)

7.14.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.14.2. The information system:

- Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
- Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

7.15. Secure Name/Address Resolution Service (Recursive or Caching Resolver) (LM)

7.15.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.15.2. If technically and fiscally plausible, the information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

7.16. Architecture and Provisioning for Name/Address Resolution Service (LM)

7.16.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.16.2. Agency shall ensure the information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

7.17. Session Authenticity (M)

7.17.1. This control is required for information systems with a **Moderate** security categorization.

7.17.2. The information system protects the authenticity of communications sessions.

7.18. Fail in Known State (M)

7.18.1. This control is required for information systems with a **Moderate** security categorization.

7.18.2. The information system fails to a known state preserving security if an information system failure occurs.

7.19. Protection of Information at Rest (M)

7.19.1. This control is required for information systems with a **Moderate** security categorization.

7.19.2. The information system protects the confidentiality and integrity of information at rest.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Information Security Team

8.2.1. Ensures pre-implementation security scans are performed on all software development projects.

8.2.2. Communicates system and communications protection security requirements with appropriate teams to ensure requirements are met.

8.3. Agency Software Development Teams

8.3.1. Works with Agency Information Security team to ensure security requirements are met for all agency applications.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes portions of P-CISP-006 Network Operations, and P-CISP-007 System and Applications Operations Policies.

The purpose of this policy is to ensure agency information systems and the information which resides thereon are protected with security controls. Implementation of appropriate security controls is based on the security categorization of the information.

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information SystemsFederal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.4. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.5. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.4. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.5. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.6. **Secure System Development Life Cycle (SSDLC):** A secure process for planning, creating, testing and deploying an information system. This includes software and hardware components of an information system.
6.7. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. Flaw Remediation (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall identify report and correct information system flaws.

- Agency shall employ automated mechanisms to monthly, and on-demand, determine the state of information system components as it regards flaw remediation.

7.1.3. Agency shall test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

7.1.4. Agency shall install tested security-relevant software and firmware updates priot to implementation.

7.1.5. Agency shall incorporate flaw remediation into the organizational configuration management process to permit tracking and verification of remediation efforts.

7.2. Malicious Code Protection (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. Agency shall employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

7.2.3. Agency shall employ mechanisms (e.g., signature definitions) that automatically update malicious code protection.

7.2.4. Agency shall update malicious code protection mechanisms (e.g., anti-virus signature definitions and reputation-based protection mechanisms) whenever new releases are available in accordance with organizational configuration management policy and procedures.

7.2.5. Agency shall configure malicious code protection mechanisms to:

- Perform checks as files are downloaded, opened, or executed; and
- Block or quarantine malicious code and notify an appropriate party in response to malicious code detection.

7.2.6. Agency shall centrally manage malicious code protection mechanisms that include planning, implementing, assessing, authorizing, and monitoring Agency-defined, flaw malicious code protection security controls.

7.3. Information System Monitoring (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall monitor the information system to detect:

- Attacks and indicators of potential attacks.
- Unauthorized local, network, and remote connections.

7.3.3. Agency shall identify unauthorized use of the information system through active and/or passive system alerts and monitoring of system events/transactions.

7.3.4. Agency shall deploy monitoring devices: (i) strategically within the information system to collect Agency-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the agency and in support of incident response.

7.3.5. Agency shall employ automated tools to support near real-time analysis of events; for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies.

7.3.6. Agency shall protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

7.3.7. Agency shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to Agency operations and assets, individuals, other organizations or the state based on law enforcement information, intelligence information, and/or other credible sources of information.

7.3.8. Agency shall obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, Executive Orders, directives, policies, or regulations.

7.3.9. The information system shall alert responsible Agency personnel when indications of compromise or potential compromise occur.

7.3.10. Agency shall ensure that the information system monitors inbound and outbound communications traffic on an ongoing basis to guard against unusual or unauthorized activities or conditions.

7.4. Security Alerts, Advisories, and Directives (LM)

7.4.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.4.2. Agency shall receive information system security alerts, advisories, and directives on an ongoing basis from external organizations such as the United States Computer Emergency Readiness Team (US-CERT), SANS Internet Storm Center, and the National Institute of Standards and Technology (NIST).

7.4.3. Agency shall generate internal security alerts, advisories, and directives as deemed necessary.

7.4.4. Agency shall disseminate security alerts, advisories, and directives to Agency personnel responsible for implementing, monitoring, and managing the information system assets.

7.4.5. Agency shall receive and review information system security alerts or advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.

7.5. Software, Firmware, and Information Integrity (M)

7.5.1. This control is required for information systems with a **Moderate** security categorization.

7.5.2. Agency shall employ integrity verification tools (e.g., information system and application integrity-checking mechanisms) to detect unauthorized changes to metadata (e.g., security attributes), software, firmware, middleware, and applications.

7.5.3. The information system shall perform ongoing integrity checks on software, firmware, and information. The integrity check can occur at a transitional state (i.e., system startup, restart, shutdown, or abort) or security-relevant event (e.g., new threat).

7.5.4. Agency shall incorporate the detection of unauthorized security-relevant changes (e.g., unauthorized changes to established configuration settings or elevation of system privileges) into its incident response capability; and ensure that detected events are tracked, monitored, corrected, and available for historical purposes.

7.6. Spam Protection (M)

7.6.1. This control is required for information systems with a **Moderate** security categorization.

7.6.2. Agency shall employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.

7.6.3. Agency shall automatically update spam protection mechanisms when new releases are available in accordance with Agency-configuration management policy and procedures.

7.7. Information Input Validation (M)

7.7.1. This control is required for information systems with a **Moderate** security categorization.

7.7.2. The information system shall validate information system inputs (e.g., character set, length, numerical range, and acceptable values) to verify that inputs match specific definitions for format and content to ensure the confidentiality, integrity and availability of the data.

7.8. Error Handling (M)

7.8.1. This control is required for information systems with a **Moderate** security categorization.

7.8.2. Information systems shall generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries (e.g., erroneous logon attempts with passwords entered by mistake as the username).

7.8.3. Information systems shall reveal error messages only to personnel having a need-to-know.

7.9. Information Handling and Retention (LM)

7.9.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.9.2. Agency shall handle and retain information within the information system and information output from the system in accordance with applicable state and federal laws, Executive Orders, directives, policies, or regulations.

7.9.3. Information handling and retention requirements shall cover the full life-cycle of information.

7.10. Memory Protection (M)

7.10.1. This control is required for information systems with a **Moderate** security categorization.

7.10.2. The information system shall implement security safeguards to protect its memory from unauthorized code execution. Security safeguards may include data execution prevention (e.g., hardware or software enforced) and address space layout randomization.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Information Security Team

8.2.1. Ensures information system monitoring occurs on a regular basis.

8.2.2. Communicates to and assists software development teams in implementing software patches and updates.

8.2.3. Ensures anti-virus protection is in place and updated regularly.

8.2.4. Performs regular scans of agency applications to ensure information system monitoring occurs.

8.3. Agency Software Development Teams

8.3.1. Follow secure software development requirements to ensure information integrity for all agency applications.

8.3.2. Assist Agency Information Security team in testing and implementing software patches and updates.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.

1. PURPOSE:

This policy is part of the State of Colorado Information Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). For the Consolidated Agencies, the Governor's Office of Information Technology (OIT) maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information. OIT documents the program details in the Enterprise Cyber Security Plan (ECSP), and sets forth security policy for the Consolidated Agencies in the OIT Information Security Policies. Non-Consolidated Agencies shall maintain an Agency Cyber Security Plan (ACSP), and implement the Colorado Information Security Policies (CISP) for the same purpose.

2. POLICY:

This version of the State Information Security Policies has been reorganized to follow the NIST SP 800-53 Rev.4 framework. The decision to reorganize Information Security Policies utilizing the NIST framework was initiated due to the amount of federal data for which the State of Colorado is custodian.

This policy supersedes P-CISP-001 Security Program Policy.

The purpose of this policy is to ensure non-consolidated agencies create, document, maintain and review an Agency Cyber Security Plan (ACSP) as defined in permanent rule 8 CCR 1501-5 (Rules in Support of the Information Security Act for the Office of Information Technology).

3. ORGANIZATIONS AFFECTED:

This policy applies to every public agency ("Agency") as defined in C.R.S 24-37.5-402(9), "public agency" means every state office, whether executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

4. SCOPE

This policy covers information technology systems with a data security categorization of "low" or "moderate". Examples of data with a security categorization of "low" include most data elements in state personnel records, building code violations, Personally Identifiable Information (PII) and firearm permits data. Examples of data with a security categorization of "moderate" include Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) and Social Security Administration (SSA).

Criminal Justice Information System (CJIS) data has a security categorization of "high" and must comply with the CJIS Security Policy.

Further guidance on data and information system security categorization levels is located in the Data Security Categorization Standard posted in the same location as the Colorado Information Security Policies –http://oit.state.co.us/ois/policies.

5. REFERENCES:

5.1. C.R.S. 24-37.5-401, et seq.
5.2. Senate Bill 08-155 as codified in C.R.S. 24-37.5-101 et seq.
5.3. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
5.4. Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems
5.5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, "Recommended Security Controls for Federal Information Systems"
5.6. Agency Cyber Security Plan (ACSP) defined in CISP-017 SP-Security Planning Policy.

6. DEFINITIONS:

For the purposes of this document, refer to C.R.S. 24-37.5-102, et seq., and the Colorado Information Security Program Policy Glossary for any terms not specifically defined herein. The Glossary is posted in the same location as the Colorado Information Security Policies – http://oit.state.co.us/ois/policies.

6.1. **CISO**: Chief Information Security Officer.
6.2. **Consolidated Agencies**: Refers to those state agencies whose IT functions were consolidated under OIT pursuant to SB 08-155 and defined in C.R.S. 24-37.5-102(4).
6.3. **Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
6.4. **Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
6.5. **Non Consolidated Agencies**: Refers to those state agencies whose IT functions were not consolidated under OIT, however, the CISO provides guidance to all public agencies as defined in the 'Organizations Affected' section of this policy.
6.6. **Secure System Development Life Cycle (SSDLC):** A secure process for planning, creating, testing and deploying an information system. This includes software and hardware components of an information system.
6.7. **Security Category**: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the state. See the Data Security Categorization standard which is posted in the same location as the Colorado Information Security policies – http://oit.state.co.us/ois/policies.

7. REQUIREMENTS:

7.1. System Security Plan (LM)

7.1.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.1.2. Agency shall develop a security plan for the information system that:

- Is consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security categorization of the information system including supporting rationale;
- Describes the operational environment for the information system and relationships with or connections to other information systems;
- Provides an overview of the security requirements for the system;
- Identifies any relevant overlays, if applicable;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

7.1.3. Agency shall distribute copies of the security plan to executive directors, and agency employees with defined security responsibilities; and communicate subsequent changes to the plan.

7.1.4. Agency shall review the security plan for the information system annually, and submit the plan to the State CISO on or before July 15th of each year.

7.1.5. Agency shall update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

7.1.6. Agency shall protect the security plan from unauthorized disclosure and modification.

7.2. Security Plan Contents (LM)

7.2.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.2.2. An Agency Cyber Security Plan shall include the following sections, at a minimum:

7.2.3. Agency Mission Objectives

- Mission Statement
- Concept of Operations
- Roles and Responsibilities

7.2.4. Information Technology Environment

- Network Environment, Enclaves, and Perimeters

- Major Applications and Systems
- General Support Systems - Define general support systems.

7.2.5. Risk Management
- Risk Assessment Methodology
- Risk Assessment Responsibilities
- Risk Assessment Frequency
- Project Lifecycle
- Vendor Management

7.2.6. Security Program
- Network and Security Operations Standards
- System and Application Security Standards
- Access Controls
- Change Control and Configuration Management
- Physical Security
- Data Handling and Disposal
- Personnel Security
- Acceptable Use
- Online Privacy

7.2.7. Incident Warning, Advisory, and Response
- Evaluating Information Security Warnings and Advisories
- Information Security Incident Response Plan Summary

7.2.8. Security Awareness and Training
- Security Awareness and Training Methodology
- Security Awareness and Training Frequency
- Security Awareness and Training Content Updates

7.2.9. Self-Assessment

7.2.10. Metrics and Reporting

7.2.11. Plan Approval and Maintenance

7.3. Rules of Behavior (LM)

7.3.1. This control is required for information systems with a **Low** or **Moderate** security categorization.

7.3.2. Agency shall establish and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.

7.3.3. Agency shall receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

7.3.4. Agency shall review and update the rules of behavior annually.

7.3.5. Agency shall require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

7.4. Information Security Architecture (M)

7.4.1. This control is required for information systems with a **Moderate** security categorization.

7.4.2. Agency shall develop an information security architecture for the information system that:

- Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
- Describes how the information security architecture is integrated into and supports the enterprise architecture; and
- Describes any information security assumptions about and dependencies on, external services.

7.4.3. Agency shall review and update the information security architecture annually to reflect updates in the enterprise architecture.

7.4.4. Agency shall ensure that planned information security architecture changes are reflected in the security plan, the Configuration Management Plan, and organizational procurements/acquisitions.

8. RESPONSIBILITIES: (ROLES AND RESPONSIBILITIES)

8.1. State Chief Information Security Officer (CISO)

8.1.1. Establish and maintain the Colorado Information Security Program (Secure Colorado), which provides guidance to public agencies.

8.1.2. Ensures successful implementation of the Colorado Information Security Policies.

8.2. Agency Information Security Team

8.2.1. Create and maintain the Agency Cyber Security Plan (ACSP).

8.2.2. Submit the ACSP to the state CISO annually on or before July 1.

9. COMPLIANCE

All State of Colorado entities identified in the 'Organizations Affected' section of this policy are required to comply with this policy. Failure to comply with this policy may result in temporary discontinuance or suspense of the operation of a public agency's communication and information resources as defined in C.R.S. 24-37.5-401, et seq.

10. EXPIRATION

This policy will remain in effect until the State CISO revises, changes or terminates it.