

RESPONSE 38e

7.6 – Security and Confidentiality Requirements	In Production? YES/NO
Description Addresses Requirements (Provide the range as applicable): 1194 – 1205, 1207, 1764	YES

HP Plan for COMMIT Security, Privacy, and Confidentiality

In RESPONSE 31, we provide a detailed Security, Privacy, and Confidentiality Plan (SPCP) that describes our proven approach to project management, risk management, project controls and other deliverables. In this section we describe our approach to implementing the security and confidentiality requirements identified for the Department’s COMMIT project.

Why the HP Approach Is the Best Solution for the Department

We will follow a defined management process for identifying security and confidentiality requirements and keeping sensitive information confidential, including Personal Health Information (PHI) and Personally Identifiable Information (PII). Our sample SPCP demonstrates our understanding and preparation to promote the integrity of the Colorado interChange Medicaid Enterprise system. Our implementation provides physical protection for facilities and associated data systems, with a plan that also incorporates multilayered electronic protection for the Department’s data.

Security control, compliant with federal and State confidentiality and security laws, will be in place on day one of the Colorado interChange launch. Protection from threats, unauthorized access, and disbursement of clients’ personal information lie within rigorous physical and operational controls.

HP will customize the SPCP to meet the Department’s RFP requirements. To provide proven value to the Department, our plans must be current, relevant, and accessible. To maximize the value of our proposal and plans, we provide tools to support access and maintenance. The illustrations below demonstrate tools we use to support other MMIS customers and will use in the COMMIT project.

Colorado Compliance Requirements (Unique ID 1194)

We will provide the Department with a Security, Privacy and Confidentiality Plan (SPCP). HP will customize the SPCP to meet the COMMIT project requirements, including applicable State and federal security and confidentiality laws, and regulations applicable to the security plan template given in Section G4.0 of the RFP appendix G.

HP will build Colorado interChange based on the proven security baseline our healthcare security experts established for 20 Medicaid accounts nationwide. Because security risks

constantly change and technology constantly advances, HP will work regularly with the Department to evolve the system and data security plans. Our team will help the Department minimize the potential effect of threats by addressing the technical, environmental, and personnel aspects holistically with a common, guiding principle. As part of the data security development life cycle, our teams will work closely with the Department to:

- Define data privacy by business area and user groups
- Define the data retention requirements
- Define the data compliance aspect of Colorado interChange

HP has extensive experience in successfully safeguarding the information for customers through documented standards, industry guidelines, and corporate oversight. HP has its own set of control standards taken directly from the industry-leading National Institute of Standards and Technology (NIST) guidelines. The NIST-800 guidelines were developed to assist technology-based companies in the healthcare industry maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. HP uses the NIST-800 guidelines as control standards to meet or exceed compliance with security, confidentiality, and audit controls. We will continue to comply with these strict control standards and work with the Department to minimize risk and continue compliance with the HIPAA Privacy and Security Rules.

Detailed Security Control Implementation and Status Information (Unique ID 1195)

Our proven approach provides defined checkpoints for Department reporting and review. Working with the Department, HP identifies clearly defined management, operational and technical (physical) controls to prevent potential threats, unauthorized access, or disclosure of sensitive information. The controls provide objective evidence to demonstrate compliance with state and federal security and confidentiality laws.

Overall Approach to Security Controls

The Account Security Governance and Compliance Management (ASGCM) tool was developed and maintained by a core group of security and privacy professionals, and provides a common and standard approach to risk management, account security governance, and compliance monitoring. The ASGCM gives the Department and HP security and privacy officers a solid platform to promote the integrity, confidentiality, and availability to sensitive information.

Documentation Repository

The Colorado interChange documentation will be organized and easily accessible for daily use and unexpected events. The COMMIT project support team will work from the interChange documentation repository that maintains and archives plan documents. By working from this accessible repository, the COMMIT project team can support routine operations and contingencies for disaster recovery and other events. The following figure illustrates the repository tools.

For the Department's COMMIT project, we will detail our plans for the entire project Systems Development Life Cycle (SDLC). Our SDLC plans are living documents, providing the Department the security and confidentiality essential for this transition. HP will work with the state to finalize the draft plans illustrated with this proposal.

Management Controls

Risk Assessment Control and Mitigation

We consistently evaluate and apply lessons learned from our previous MMIS projects and add these to our repository of best practices and lists of known issues and risks. By consistently improving best practices, our team can proactively mitigate risks. We discuss these risks with the Department during requirements validation sessions or risk review meetings, prepare mitigation plans and promote a smooth implementation.

HP will implement the risk assessment template recommended in NIST 800-30 and assess the effect periodically to minimize or to eliminate the loss. The status information of the new threats that are anticipated and reported in SANS.org will be carefully analyzed periodically, and HP will implement pro-active measures to avoid disruption to confidentiality, integrity and availability.

Initial Risk Assessment

During the Start-Up Phase, the HP team executes an initial risk assessment. Part of this risk assessment is to review the risks with the Department to verify that we have captured the possible risks and mitigation steps. Risk analysis produces an assessment of the loss probability and loss magnitude associated with each identified risk. The team analyzes risks in terms of the probability of the risk occurring with an unsatisfactory outcome and the effect of the risk to the stakeholders. Also, as part of the risk management plan, the team works with the Department to confirm the description of the probability and impact rating scales before risk assessment. We import this information into the HP Account Service Governance and Compliance Management tool as part of the mechanism of risk qualification. The risk level for each risk determines the expected project effect and the prioritization of risk-reducing responses developed in subsequent stages of the risk mitigation process.

System and Service Acquisition

If the Department has a business need to expand and requires additional hardware or software, the HP team initiates a Request Fulfillment to engage the appropriate group within HP. Each group follows a set of HP guidelines assuring compliance to both industry standards as well as State and federal security and confidentiality laws. The change control process includes peer reviews during development, review by a change advisory board, and review by a security administrator before implementing into a production environment.

Risk and Mitigation Strategy

Risk management is the process of identifying and assessing risk, taking steps to reduce risk to an acceptable level, and monitoring implemented security controls to confirm they continue to

operate effectively and as intended. HP risk management uses a process that allows HP to balance the operational and economic costs of protective measures. This method achieves gains in mission capability by protecting the Department's assets that support delivery.

Key roles defined by HP provide the foundation for risk management, reducing risk to the Department to an acceptable level and monitoring implemented security controls to confirm they continue to operate effectively and as intended.

Owners

System and information owners are responsible for confirming that proper controls are in place to address confidentiality, integrity, and availability of the information systems and data they own. Typically, the system and information owners are responsible for changes to their information systems. Thus, they usually have to approve changes to their information systems—such as system enhancement and major changes to the software and hardware. The system and information owners must, therefore, understand their role in the risk management process and fully support this process.

Custodians

System and information custodians are users and administrators of the information systems. Use and administration of information systems and data according to the Department's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the Department's information system resources.

Privacy and Security

IT security practitioners—such as network, system, application, and database administrators; computer specialists, security analysts, and security consultants—are responsible for proper implementation of security requirements in IT systems. As events such as expansion in network connectivity, changes to the existing infrastructure and organizational policies, or introduction of new technologies occur to an existing IT system environment, privacy and security practitioners must support or use the risk management process to identify and assess new potential risks. If this occurs, HP team will implement new security controls as needed to safeguard IT systems.

Policy Testing

HP also uses policy testing to mitigate risk. As a best practice, we developed and refined a policy testing approach and supporting tools specifically for interChange implementations. Our policy testing shows the progress achieved to deem the system ready for production processing. Policy testing allows us to verify that Colorado interChange adheres to the COMMIT project's claims processing policies and procedures. Regardless of the differences with the legacy system and policies, our policy testing verifies the accuracy and consistency of outcomes between the current claims processing systems and Colorado interChange.

Policy testing helps to verify that we are paying claims correctly. During policy testing, we validate and confirm the differences and that provider payments are accurate. This verifies that

we consistently apply the policy as we transition, giving the Department confidence to proceed to the Operations Phase.

Certification Planning Risk Mitigation

HP also applies risk mitigation during the certification planning process. The certification readiness plan includes a communications plan and comprehensive risk management protocols that provides the structure for problem identification, tracking, resolution, and reporting. A key feature of the HP Certification Readiness plan is a risk-reduction process that enhances the overall enterprise risk management process. We have discovered that a no-blame, positive approach to the identification and correction of system defects, through frequent checkpoint sessions, results in an efficient implementation and, ultimately, a successful CMS certification review.

The HP audit process will verify that hardware and software components are part of the HP Tech Policy of methodology. HP Tech Policy covers qualified and certified components reducing the risk of implementing non-compliant components.

As Colorado interChange moves into the Fiscal Agent Operations Phase, we diligently monitor our own performance. The HP team proactively monitors system availability and operations, which includes comparing and evaluating actual system performance to system specifications and initiating resolution of anomalies. We build our team to appropriately support and monitor the MMIS as we have done successfully and satisfactorily in our other states. The interChange inSight Dashboard provides complete transparency into the system, operational, and program metrics. Having the metrics available through a single dashboard portal will provide a “one-stop shop” approach to monitoring the system. The features of the interChange Insight dashboard include the ability to proactively notify key stakeholders when predefined performance thresholds are eclipsed. Thus, the Colorado interChange solution goes beyond reporting metrics and uses the metric parameters to actively manage the business. Cross-training and knowledge-sharing occur continuously within the teams. This avoids single points of failure and reduces the risk of service disruption when key personnel are unavailable. We also stagger teams and team members to provide an effective 24 x 7 support rotation where applicable. We schedule employees within each critical support team on a production-support rotation in which different members of the team would be on call at different times.

Planning

As part of our Management Controls, the Performance Management Plan, a subsidiary plan to our Project Management Plan, documents the following measurement responsibilities:

- What to measure (metrics)
- When to measure (frequency)
- The level of data summarization (granularity)
- The data sources
- The destination of the collected data

The plan also describes the frequency of metrics analysis/reporting and defines corrective action triggers. The Performance Management process includes capturing, compiling, and reporting contract performance measures and metrics to the Department to confirm we meet contractual requirements.

Systems and Services Acquisition

HP brings a structured framework for project activities that define the right work and the right way to do it. HP verifies the work defined in the project schedule accomplishes the project plan and meets the business need, addressing the Department's goals. Our project management approach follows the *Guide to the Project Management Body of Knowledge* (PMBOK) and addresses the primary constraints on a project—cost, scope, schedule (time), and quality. The PMBOK considers these basic conditions' constraints because they set the limits or boundaries on projects. The constraints provide the parameters used to achieve success and include:

- **Scope**—A written statement that defines the project (the RFP). The scope statement is used as the foundation for scope and project schedule refinement during project planning.
- **Schedule (time)**—A preliminary project schedule defines the activities that must be accomplished at certain points in the project to deliver the product described in the scope.
- **Quality**—The quality evaluation processes and standards are used throughout the project.
- **Cost**—The appropriate approach to staffing and materials acquisition is used.

Certification: A MITA-Aligned Solution

We designed the new CMS certification protocols for provider management to assess the degree of MITA alignment achieved by our business areas and technical processes. We continue to develop our MITA-defined MMIS business functions for provider management to highlight this alignment and validate we can meet current and future checklist requirements. Additionally, the Department's path to achieving higher levels of MITA consistency should continuously improve.

The underpinning of our approach to MMIS certification is end-to-end traceability; so there is no doubt how we have “proven” the system. The Colorado interChange solution is CMS-certified, which emphasizes that HP delivers a certified solution—not merely a “certifiable” product.

Accreditation and Security

HP employs more than 2,500 security and privacy professionals worldwide. HP has seven ISO27001 certifications and supports 36 ISO27001 certified organizations staffed by 8,000. There are 1,242 security certifications in 76 unique security accreditation areas held by HP staff.

Program Management

Colorado interChange offers a single, unified dashboard—interChange inSight—that reports on system, operational, and program management metrics. We use multiple review methods and data analyses to monitor and measure the HP team's operational performance. Areas we monitor

include claims processing and adjudication, provider and member relations, financial processes, and training.

The HP leadership team, our Project Management Office, and quality managers have defined standard performance measurements that tie back to contract requirements. We apply ongoing quality checks and corrective action to improve results. Our goal is to provide thought leadership, not just fulfill requirements or meet SLAs. Our quality management staff will work with the Department to capture and report metrics that are meaningful to the Department.

Operational Controls

Personnel Security

The Department and HP facilities' surrounding grounds are the first line of defense for protecting information, assets, and staff members. HP designs the facilities to limit access to only authorized personnel. We lock unmanned entrances to prevent unauthorized access. Our physical facility access protocols include the following security measures, guarding against intrusion and unauthorized use of system resources:

- Security badge entry cards and unique PINs
- Cameras at access points
- Escorts
- Hours of access
- Mechanical audit logs and monitoring stations
- Policies for background and security clearance
- Fire suppression and flood warning systems, fuel, and battery backups
- HVAC control and network drop access
- Zoned Access

HP designs our facilities to limit access to authorized personnel only. An HP work force member will watch the reception area and have visitors sign the Visitor log before granting access. We lock unmanned entrances to prevent unauthorized access. Facility exteriors and the surrounding grounds will be well lit, including the parking areas and walkways.

Zoned Access

HP facilities have security controls that physically separate various zones, which require different types of permissions with varying access card credentials, door codes, or combinations to gain access to more restricted areas. Control points include at a minimum:

- Main entrance to the information processing and claims processing facilities
- Service entrances

The Wisconsin Medicaid program was the first to use the new CMS checklists for CMS certification, and to be certified back to day one. The new checklists feature 38 requirements and hundreds of validation points for provider management. We scored perfectly on each one.

Our successes in Wisconsin were made possible by an industry-best system, architecture, and network. CMS recognized the Wisconsin MMIS and its corresponding business processes for more than 250 industry best practices. Further, the HP Georgia MMIS was the first MMIS in the country to be reviewed for adherence to the new CMS certification checklist and certified within 12 months of implementation.

- Loading platform or garage entrances
- Inside entrance to the facility
- Secondary entrances

In cases where unauthorized personnel, such as maintenance or cleaning personnel, network providers, or visitors need access to secured areas, an authorized person must accompany them and monitor their activity.

A security badge system controls access and the days and times the badge holder can be on the premises, dependent on the staff's job responsibilities.

HP will designate areas within the facility with access levels. This includes areas open to staff, areas open to Department staff only, and restricted areas. Restricted areas include equipment/telecommunications rooms.

The Department-designated office space will have the same security features as the HP office space described previously. HP is committed to providing a safe and secure work environment. HP will designate areas within the facility with access levels. This includes areas open to staff, or to the Department staff only, and restricted areas. Facilities used by Department staff will be designated as Department staff areas and entrance to the Department's designated areas will have badged access. The Department will review and authorize access to Department designated areas.

Key Cards and Visitor Logs

As part of the physical security controls, visitors, including messengers, will be required to sign the visitor log before receiving a temporary badge. HP expects visitors to have identification or credentials. An HP employee will watch the reception area and have visitors sign the Visitor log before assigning the visitor a visitor badge.

The information in the visitor log will include at a minimum:

- The visitor's name
- The agency/company the visitor represents
- The purpose of the visit, including name of individual to whom the visit is made
- Date and time of arrival
- Date and time of departure

An HP or authorized Department staff member will assign visitors a visitor badge and escort them to their destination. When visitors leave the facility, they surrender their visitor badge.

Physical and Environmental Protection

We propose the Orlando (Fla.) Data Center (ODC) and the Colorado Springs Business Continuity Recovery Services (CO BCRS) to house the COMMIT project production and failover environments respectively. These are two of our strategic facilities available for state and local government data center hosting services. The ODC facility will host both the production and test/development environments in separate compartments. The Colorado Springs

Facility will serve as the disaster recovery site. Both facilities are immediately available to serve the COMMIT project.

Orlando Data Center

The HP Orlando Data Center (ODC) meets the requirement of a “data center with computing environments operating at a commercially available grade”. The ODC is a purpose built SSAE-16 Certified facility that consists of 85,000 square feet of 36” raised floor with reinforced concrete walls, dual power feeds and air conditioning systems and redundant generators that can run for 72 hours.

These services are structured to meet U.S. Department of Defense (DoD)/Federal Certification & Accreditation (C&A) for multiple agencies, as well as Federal Information Processing Standards (FIPS).

The facility is staffed 24 x 7 with security personnel and has two factor access controls with extensive video surveillance. A monitored two stage dry pipe pre-action fire suppression system, with smoke detectors in all areas above and below the raised floor, verifies that fires are quickly detected and extinguished.

Network management services provide a variety of secure communication protocols with redundant access to Customer networks, HPQnet and the Internet across multi-vendor communications. The ODC offers managed storage including Tier 1 storage area network, Tier 2 network attached storage and Tier 3 SATA/FATA. This enables HP to meet the storage requirements for our customers.

HP’s Orlando facility supports customers at NIST moderate levels by default.

The ODC is designed to meet the requirement of a Tier III data center operating as a purpose built facility with complete redundancy that has seen a 100 percent uptime record during the last 10 years. While the ODC is classified as a Tier III data center, it meets most Tier 4 requirements. It is fully redundant with sustainable power and cooling to maintain maximum availability and uptime:

- Fault-tolerant site infrastructure design and implementation capable of withstanding electrical power, cooling fluctuation and disturbances
- Redundant power and distribution for network devices, servers, equipment and components
- Multiple independent distribution paths for network devices, servers, equipment and components

The following graphic contains tier criteria and highlights the ODC’s Tier 3 and Tier 4 capabilities.

RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED

The ODC was specifically designed with our healthcare customers in mind, adhering to government security standards while permitting smooth and efficient connectivity for the State, agencies, and external organizations. Our end-to-end reach and services include design, installation, testing, maintenance, and ongoing management. We can provide the latest technology in a proven, shared environment without risk, uncertainty, high capital expenditures, or commitments to particular equipment.

HP uses existing infrastructure, shared assets, and resources. This shared infrastructure and shared assets pool resources in a single chassis and spread them among independent server nodes within that same chassis to achieve optimized performance.

There are many advantages of a shared infrastructure that shares existing assets:

- Elimination of the acquisition or purchase of a datacenter; maintenance and management
- Reduced compute density through shared assets
- Reduced operating costs through efficient use of resources
- IT Infrastructure Library (ITIL) compliance
- Application of industry best practices
- Immediately availability

Space

The ODC is a world-class data center facility designed to meet the demanding power and cooling needs of the modern computing environment. The facility is scalable and immediately available.

The facility has infrastructure in place today to house, power, and cool any hosting requirements needed to run the COMMIT project. Some features of the facility include the following:

- 130,000 square foot purpose-built fortress
- Two high-voltage sub-stations on diverse grids
- Jet turbine generators
- 85,000 square feet of 36-inch raised floor
- 24 x 7 on-site security
- Extensive video surveillance systems
- Water-cooled equipment supported
- Remote hands services available
- Metered power
- 36-inch raised floor
- Dual concrete encased fiber duct banks
- Cabinets, cages, or private suites built to meet specific requirements



Located in an 18-acre safe haven that provides a secure private environment, the facility is designed to run continually, as it has for the past 10 years

Power (Primary and Redundant AC/DC)

The ODC provides uninterrupted power to tenants on the raised floor with dual 12.4-kilovolt power feeds from a diverse array of utility substations. Multiple UPS and battery rooms powered with turbine jet engine generators provide backup during a power outage.

The facility houses the following devices for uninterrupted service:

- Two separate 12.47-kilovolt underground service feeds
- Two diverse high-voltage utility substations
- Double-ended main switchgear with tie breaker
- Double ended distribution switch gear with tie breakers
- Multiple diverse UPS and battery rooms
- Three 2.8-megawatt turbine jet engine generators
- 40,000 gallon underground fuel tanks

Cooling

The HP ODC Facility is equipped to meet cooling requirements for current and future hosted environments. Cooling is regulated, with hot and cold aisles for optimal operation and efficiency. The ODC can deliver cooling capacity that surpasses 500 watts per square foot of power consumption. Cooling features include:

- 2,750 ton centrifugal chiller plant
- Four 1,500 GPM Marley stainless cooling towers
- High capacity deep water well with 10,000 gallon holding tank

- Fifty-two 20 ton computer room air handlers installed on raised floor
- Chilled water loop available for water-cooled equipment

Colorado Springs BCRS

HP proposes the HP Recovery Center for our disaster recovery site in Colorado Springs, just east of the Rampart mountain range. This is a stable, protected area free from most natural disturbances that can affect business, and located separately from our main production center in Orlando.

HP's 360-acre Colorado Springs site is ideally suited to house data centers that support disaster recovery and the nonstop computing and networking service businesses.

Physical access and security to the building is tightly controlled. Full-time, dedicated personnel oversee the security of the campus. Security monitoring is provided by physical walk through checks, along with extensive video monitoring of the facility. Electronic and visual badge verification is maintained at all hours. Around-the-clock monitored badge access limits entry to data center and the rehearsal room. In the following table, we show the Colorado Springs Recovery Center Specifications and the physical center's construct.

Recovery Center Specifications

Location	Colorado Springs, Colorado
Tier Level	Tier II - has multiple power and cooling distribution paths, redundant components, concurrently maintainable
Floor-space	25,600 Square feet
Humidity Controls	Relative Humidity at approximate 50 percent
Temperature Control	Approximately 75 degree return air
Fire Resilience	Two-hour fire-rated partition and doors
Staging Facilities	Customer dedicated staging rooms that enable server pre-installation with minimal risk to the operational environment
Office Space	Office and conference room space is available to customer engineers for administrative duties
WAN Connectivity	Time Warner, AT&T, Verizon
Internet Access	Time Warner, AT&T, Verizon

HP provides world-class data centers designed to meet the demanding power and cooling needs of the modern computing environment. These chosen facilities, the ODC and the Colorado Springs BCRS has infrastructure ready today to house, power, and cool any hosting requirements needed to run the COMMIT Project.

Our team has successfully transitioned multiple MMIS solutions, state Electronic Benefits Transfer (EBT) systems, and other state and local government data center hosting solutions into these facilities.

Contingency Planning

The Risk Assessment Plan identifies contingency plans besides other risk mitigation plans. Contingency planning comprises the steps we take if a risk happens. We require contingency plans for risks prioritized as High (Red) or Medium (Yellow) and the risks where acceptance is the only action taken. Contingency planning moves the project from a reactive to a proactive mode of operation.

Escalate Risk

The work group may escalate a risk per the governance process. This may occur throughout the risk management process based on the need for approvals or urgency of the risk.

When the team escalates a risk, the reason is documented in HP PPM. This will help project leaders understand the reason for escalation. Escalated project risks are reported in the project management status report and accessed in HP PPM as seen in the next figure.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

Execute Risk Action (Contingency) Plan

Following the analysis of potential risks, we create risk mitigation and contingency plans for medium- and high-severity risks. When created, we link these plans and the associated risks directly so that they are available to appropriate users for review. We develop risk action (Contingency) plans in response to the identified risks.

The HP team uses MMIS historical information from previous implementations and MMIS knowledgeable personnel to identify and present the best risk mitigation strategies. Each risk identified in the Risk Assessment Plan is assigned a “risk owner.” The risk owner is typically responsible for the execution of the contingency plan(s).

A contingency plan includes information on the following:

- Description of the actions to be implemented
- How the actions mitigate the risk's effect on the schedule, cost, resources or quality
- Determination of the timing of the risk—what phase of the system development life cycle

The risk owner will identify in HP's Account Security Governance and Compliance Management tool the timing of the risk event to determine when the contingency plan needs to be implemented. After the work group and the Department project manager have approved the contingency plan, the risk owner develops the contingency plan for the assigned medium- and high-severity risks.

If the risk occurs—that is, the risk is realized—then a contingency plan will be implemented. The action plans created in the “Develop Risk Action Plan” step for contingency plans are now executed. The risk owner is responsible for executing the contingency plans.

The risk owner tracks the status and effectiveness of the risk mitigation and contingency plans. The plans are visible to appropriate users within HP. Regular risk reporting occurs in weekly status meetings, work group meetings, and risks are reviewed in specific risk review meetings.

Configuration Management

The configuration management plan describes the configuration management processes and activities. The configuration management plan includes planning of configuration management, configuration identification, configuration control, configuration management reporting, and baseline verification, including auditing. The final draft plan also identifies the roles and responsibilities for configuration management.

Maintenance – Security Patches (Unique ID 1203)

HP security standards confirm that the most current level of corrective and preventive patches is applied, providing a proactive approach to securing and managing the environment. HP will notify the Department of the receipt of security patches within 24 hours of receipt of the patches.

Colorado interChange will have availability 24 x 7 except for scheduled maintenance. HP will implement a structured approach to updating systems with minimal effect on program stakeholders. This includes the Department business functions and the system users. HP will work with the Department to determine the most appropriate time for necessary installations and upgrades to Colorado interChange and its components. We will schedule these maintenance windows with Department approval for a time when program and Colorado interChange activity is at a minimum.

As part of the documented communication process regarding system maintenance, HP will inform the appropriate stakeholders using the methods defined in the maintenance plan.

System and Information Integrity

Project Level

The configuration management methodology outlines the process and tools used to control project assets and work products. The methodology supports a formal change control process required when a configuration item is changed. HP's configuration management methodology will provide the COMMIT project with a rigorous, repeatable process based on industry standards and our Healthcare Enterprise EDGE Process Framework for SDLC methodology. Although our approach begins with our methodology and standards, we customize it for the Colorado interChange environment. The following are the major components of configuration management:

- **Management and planning**—Establishing and maintaining the integrity of the project assets and work products; and defining the configuration management processes and activities that establish and maintain administrative control of project data
- **Configuration identification**—Identifying the configuration items, components, and related work products that we place under configuration management
- **Configuration control**—Tracking the configuration of each of the configuration items, approving a new configuration if necessary, and updating the baseline
- **Configuration status accounting**—Recording and reporting the configuration process with the goal of maintaining a status record of items in the baseline, thus providing traceability of the changes
- **Configuration verification and audit**—Auditing to confirm that the resulting baselines and documentation conform to a specified standard or requirement

Application Level



An integrated security framework manages access and exchange of information deployed across the applications helps support privacy, control data integrity, and manage role-based access and authentication to the proper applications, panels, and data. Colorado interChange provides role-based security access across the MMIS solution. The role-based security access enables various levels of security, as defined by the Department, for Colorado interChange.

We grant access on a defined need basis, with business groups having profiles established within the security solution. As we add Colorado interChange users, we authenticate and authorize them according to their defined and assigned profile. This role-based approach limits the access to the specific business areas, the specific online user panels, and the specific features—add, update, or inquire—of the user panels, as needed, to maintain proper security.

The same security framework manages web portal access and authorizations granted to each specific user. For providers, the security solution enables them to establish delegates to support the standard business models used by provider offices, where the office staff members routinely

enter prior authorizations, eligibility requests, and claim submissions. Each of the delegates has an individual ID and password, and the provider can authorize the delegate for all or a subset of the provider's access. Self-initiated password resets minimize the need for help desk interaction. HP has employed the use of this role-based security approach across our many solutions to the benefit of the secure MMIS.

Media Protection

Off-Site Storage Procedures and File Backup

HP uses Iron Mountain off-site storage facilities that protect the backup media against unauthorized access, disclosure, or sabotage. A fireproof storage unit for backup media protects against fire or other environmental hazards. Additionally, we maintain a second copy at our disaster recovery site on disk that is replicated, near real-time, from our primary site. Our retention approach begins with daily on-site backup copies kept on disk and tape. We use disks to facilitate our recovery responsiveness, while the tape copy guards from unintended deleted disk copies. Our process includes these steps. We make one snapshot copy daily of the primary storage and keep it for 24 hours. The following day, as that day's snapshot copy is transferred to disk, we snapshot-release the previous disk copy. We keep the on-site tape copy of the first snapshot until we successfully create the on-site tape copy of the third snapshot. This approach verifies that we always retain two days of backup copies and enables us to support the Department immediately at an off-site location (Iron Mountain) if a disaster occurs. We maintain two weeks of backup copy tapes at Iron Mountain.

Incident Response

Under HIPAA, 45 Code of Federal Regulations (CFR) 164.308(a)(6)(ii), 45 CFR 164.530(f), and section 13402 of the HITECH Act, each employee at the Colorado interChange account is trained as required to assist in preventing, protecting, and reporting security incidents—including hacking and intrusion. The HP Global Security Group (GSG) leads in the investigation of incidents to determine if unauthorized access occurs. If unauthorized access to customer personal data occurs, the HIPAA compliance officer consults the HP Privacy Office. Our policy is to report customer data breaches to our customers and law enforcement officials based on the requirements in the specific customer contract, relevant security breach laws, and regulations. We have cross-functional, multidisciplinary escalation processes to proactively manage security incidents. HP provides security incident reporting and mitigation mechanisms such as the following:

- Warning or reporting about system activity based on security parameters
- Terminating access or generating report after detection of a potential security violation
- Preserving and reporting specified audit data after detection of a potential security violation

HP defines an incident as an unplanned interruption to IT Service or a reduction in the quality of IT Service. HP uses the Incident Management process to manage IT service disruptions and restore regular service operation as quickly as possible. The overall goal is to minimize adverse

effects on the COMMIT project's business operations. We provide detail on HP's Incident Management process and seven sub processes in RESPONSE 39e. The Incident Management process focuses on the rapid restoration of regular service operations, minimizing the effect on your business and the COMMIT project users.

Our post-breach review procedure includes the analysis of system and procedure weaknesses to validate that we take appropriate remedial and longer-term cause elimination efforts. A successful breach notification plan encompasses more than just a method for promptly notifying the victims of a security breach event. HP will implement full audit trails of system activity so that when a security breach occurs, the mechanism and extent of the breach can be determined. We will help the Department minimize the potential effect of threats by addressing the technical, environmental, and personnel aspects holistically with a common, guiding principle. HP requires that we maintain an audit trail of security relevant events. These events include the following:

- Network access attempts
- Database start-up and shutdown
- Creation, alteration, and deletion of user accounts
- Unsuccessful attempts to connect to the database
- Activity performed by users with elevated privileges

Security Awareness and Training

HP requires staff members to complete mandatory periodic training in privacy, confidentiality, computer security awareness, and accepted computer security practices for employees. This includes contractors, temporary employees, and permanent contractor employees.

Besides the HP Corporate Security Training Program, as part of this Security, Privacy and Confidentiality Plan, the HP HIPAA Compliance Officer will develop and implement a Colorado interChange account security, privacy and confidentiality awareness program. This program requires employees who have responsibility for information processing equipment and the handling or processing of or the exposure to confidential data to participate in the training. After initial training is complete, HP will establish an ongoing security program. At a minimum, the program will contain following basic elements:

- New employee and on-site third party work force account-specific security and confidentiality training. Employees must complete this before contact with any PHI, PII, or other sensitive information or within one week of hire, whichever comes first.
- On completion of training, new employees and on-site third party work force will be required to sign an acknowledgment statement. As with the new employee training, users must complete this before contact with any PHI, PII, or other sensitive information or within one week of hire, whichever comes first.
- Additional role-based training, as appropriate, such as system administrator security training is required.

- Distribution of periodic security and confidentiality bulletins to the account work force. The bulletins will provide general information on corporate privacy, security policies and procedures; and external privacy and security news of interest to the account work force.
- Distribution of security and confidentiality alerts. A privacy/security alert is to be issued on an as-needed basis in response to a known or suspected privacy or security event or threat. Its purpose is to provide timely information to the account work force to avert or mitigate a privacy or security event or threat.
- Posting security, privacy and confidentiality reminders in the workplace. Reminders will be posted in conspicuous locations or specific work areas (such as conference rooms) and include information on recommended security and confidentiality practices.

HP bases the appropriate amount of account security, privacy and confidentiality training on the information systems to which personnel have authorized access. This training will, at a minimum, include the following topics:

- Federal and state laws related to security and confidentiality that apply to the work performed for Colorado interChange, including HIPAA, and National Institute of Standards and Technology (NIST).
- HP's security, privacy and confidentiality policies and procedures developed to comply with the applicable state and federal laws, including acceptable use, access, and data protection.
- Classes include topics on sensitive information, such as PHI, PII, proprietary information, public information, and information that is exempt from disclosure under public record laws.
- Staff's roles and responsibilities in maintaining the security and confidentiality of sensitive information and preventing unauthorized disclosure by practicing formal security and confidentiality procedures, such as proper password usage, including creating, changing, and safeguarding passwords.
- Education on how security and confidentiality breaches can occur in everyday work practices and what steps can be taken both by individuals and by automated processes to minimize or prevent these breaches. Examples are preventing attempts at social engineering by not opening email attachments from unknown sources, notifying the Global Security Group (GSG) of attempted phishing, and not forwarding emails suspected of containing viruses.
- A review occurs for the manual and automated processes used for the Colorado interChange MMIS and the policies and procedures to protect these processes.
- Physical safeguards for the building will include fire safety training.

Training for the Department will use concrete examples of information created, maintained and used, both in paper format and by automated/electronic processes.

Each leader will be responsible for verifying that every new employee receives and reads the training documentation and certifies that they have completed this training. Leaders are responsible for answering employee questions, or referring them to the appropriate resource to answer their questions. After the training is complete and certified, the leader will route the signed document to the HP Colorado HIPAA Compliance Officer for review and recordkeeping.

Technical Controls

Identification and Authentication

Each user has a unique ID to access the system. Colorado interChange allows the individual user to access applications on the system only if the user enters the correct user ID and password. User IDs are set up with role-based security, with the ability to assign multiple roles to a user ID. This means the system limits each user to his or her authorized functions.

Our solution supports a user security profile to control user access rights to appropriate levels of functions. For example, some providers may have inquiry access only while others will have the update capability necessary to submit claims. We do not provide stakeholders access to a part of the system they are not required to use. The logon process provides a list of applications available. The user sees only their authorized applications listed on this screen.

Access Controls

HP will provide access controls at several levels: physical, network, platform, application, Internet, and web services. Physical access controls restrict access to the media where the data is stored and prevent physical destruction of the media.

The network controls are for the network resources and related functions and policies. This includes hardware such as routers, firewalls, and DNS. Operating platforms and individual applications have internal access controls. Third-party tools work with internal access controls to enhance capabilities. We will employ third-party tools, such as Microsoft Active Directory single sign-on (SSO), Lightweight Directory Access Protocol (LDAP), and industry-standard protocols, such as SAML. Access controls support privileged users and groups, separation of duties and policy enforcement on application access. Internet and web services also have internal controls and work with third-party tools to enhance capabilities.

Audit and Accountability

We will build Colorado interChange on the proven moderate- to high-security baseline our healthcare security experts have established for our Medicaid accounts nationwide. Because security risks constantly change and technology constantly advances, HP will work regularly with the Department to evolve the system and data security plans. HP uses the NIST-800 guidelines as control standards to meet compliance with security, confidentiality, and audit controls. We comply with these strict control standards and work with the Department to minimize risk and maintain compliance with the HIPAA Privacy and Security Rules.

The Colorado interChange web-based interface expedites manual entry of member-related data that external interfaces do not provide. Colorado interChange tracks updates to member and eligibility data through batch, real-time external interfaces, or web panels, allowing a complete audit and reporting process. The audit trail records the action performed (insert, update or delete), date of the change, the source of the change (electronic file or staff ID making the change), and what information changed because of the update, providing a clear view of the change history of the data. Each functional area of HP's interChange solution has an audit trail function. Colorado interChange solution supports the capability for the correction of data and the correct display of information for clients whose eligibility has been changed retroactively. The following figure shows the Client Benefit Plan and Medical Status Code Audit panel.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

System and Communication Protection

Data Transmission

We will implement several design and configuration solutions to secure how to transfer data between HP and the Department, as well as between HP sites. At a minimum, data on any medium that we physically transfer between physical sites will meet the HP Information Handling Policy.

Our electronically transmitted data solution always promotes the privacy and confidentiality of sensitive and confidential data. HP can support a variety of methods to help promote the privacy and confidentiality of information transfer. Data transmissions containing sensitive or confidential data will take place using one or more techniques to facilitate privacy.

In the following list, we identify some of the approaches we support for private and confidential data transfer:

- Secure hypertext transfer protocol (HTTPS)
- Dedicated circuits or VPNs
- Secure file transfer protocol (SFTP), which requires HP and the submitter/receiver to use encrypting routers

HP will work with the Department and outside entities to achieve secure communications for files and data received and sent as interfaces to Colorado interChange.

Additional protection from unintentional disclosure of data to an unauthorized party will include software and systems designed to prevent and report the transmittal of specific data elements that violate policies for that specific data type. We will configure computer operating systems based on policy to recognize specific types of devices and only perform actions specific to that type of device. We will work with the Department to define appropriate redaction policies before printing reports or displaying data.

Encryption

HP can apply encryption at three levels:

- **Storage**—Mechanism using hardware or software that will encrypt the data stored on the backup media
- **Network**—Object Management Group (OMG) hardware and or software solutions for data traveling across a network or the Internet using an encrypted network session
- **Application level**—Proprietary encryption capabilities built into the application if deployed in a secure environment

Additionally, End Point Threat Management Software keeps HP PCs and servers clean from viruses and malware.

Communications Protection

Staff will be required to encrypt email containing PHI/PII or other sensitive information before sending. We will provide the appropriate software such as S/MIME to encrypt email communication. HP will train staff on:

- How to use the secure email
- How to determine if the email should be sent as secure email
- How to securely archive email

To maintain comprehensive security, HP uses a layered approach or layered defense. HP designs communication switches and network components outside the central computer room and computer, telecommunications rooms, or wiring closets appropriately to prevent unauthorized access. If unauthorized personnel need access to secured areas, an authorized person must

accompany them and always monitor their activity. We designate areas within the facility with access levels. The keycard controls the cardholder's access to areas within the facilities.

HP recognizes the importance of protecting the data entrusted to them by the Department. One of the many layers of protection is preventing unwanted users and traffic on the network. This layer of security includes such actions as network and host intrusion detection and intrusion prevention, service and protocol filtering at points such as a firewall, and following standard practices to harden servers.

Network Intrusion Detection (NIDS) protects critical information assets from existing and emerging threats and unauthorized access. This service helps reduce costs and network downtime, as well as provide 24 x 7 monitoring by highly trained network specialists.

HP will implement TippingPoint as one component of a layered network security approach. We strategically place sensors at critical network points with specific inspection criteria to examine defined traffic flows. The service uses standard vendor baseline inspection criteria and environment-specific criteria derived from the initial and ongoing status of the environment.

In the Intrusion Detection component of the offering, the alert process activates when traffic flow is identified as inappropriate according to the preset criteria. The alert process defines the steps to advise the appropriate personnel for possible additional analysis or corrective action.

Application Functional Capability (Unique ID 1196)

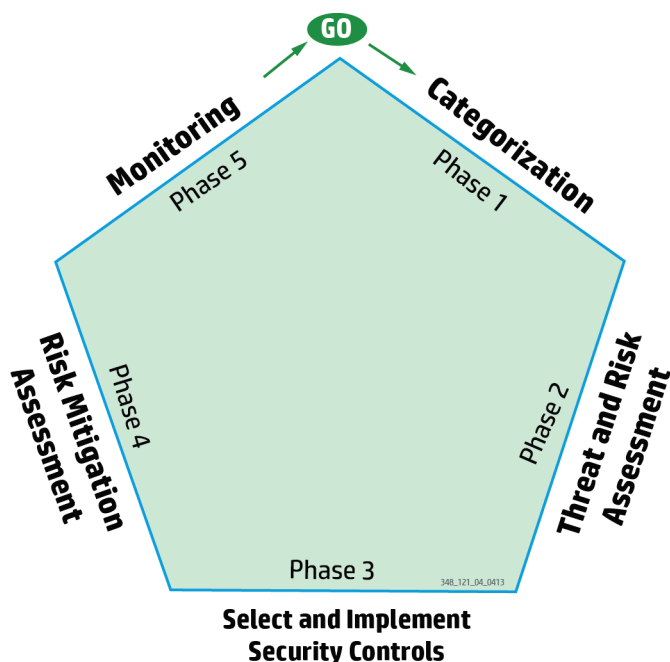
During system verification and validation, HP documents that the implementation of infrastructure, software, communication, and security requirements according to defined and documented security and functional requirements.

Security Control Functional Capability

We focus on actions supporting increased confidence in the correct implementation and operation of the control. An essential part of the control includes specific capabilities and documentation demonstrating that the control meets its required function or purpose. Auditors use this documentation to analyze and test the functional capability of the control.

In the following figure, the Monitoring Phase reviews the documentation produced by the control during the Select and Implement Phase.

Phases in the Risk Management Lifecycle



Confidentiality, Integrity, Trust (Unique IDs 1197, 1198, 1199)

(1197) The ESPS/Access Policy provides access to HP information, assets, and resources, including those entrusted to HP by third parties. Access is authorized, controlled, and monitored based on job-related function and need-to-know criteria.

ESPS combines security best practices and expertise to deliver policies, requirements, control standards, implementation procedures, release of artifacts and system code. HP's comprehensive security policies and standards are maintained in a hierarchical structure composed of four levels.

(1198) HP's staff will not disclose Department sensitive or confidential information to anyone other than the Department without prior written authorization from the Department program contract manager, except if state or federal law requires disclosure. HP's staff will promptly transmit to the Department program contract manager requests for disclosure of any Department sensitive or confidential information—including PHI/PII or other sensitive information not emanating from the person who is the subject of the information.

(1199) Consistent with the confidentiality provisions of the contract, HP will not disclose confidential information unless permitted by the confidentiality provisions or otherwise required by law.

Colorado's Address Confidentiality Plan (Unique ID 1201)

The HP Security team has reviewed the Colorado Address Confidentiality Plan. HP will work with the Department to confirm that the data affected is protected in compliance with the statute. We will implement this provisioning with the business rules engine.

Third-Party Cyber Security Assessment (Unique ID 1202)

To help verify the Colorado interChange MMIS solution meets defined architectural, performance and security requirements, HP will retain an external third party to execute the security audit before the system enters production use.

Role-Based, Single Sign-On User Access (Unique ID 1200)

HP has developed a framework that enables the overarching solution to stay platform neutral and use web services. The security architecture encompasses a large array of subcomponents, each playing a role in integrity by controlling access to resources and keeping the system safe from fraudulent or malicious intrusion.



The standard in Service Oriented Architecture (SOA)-related security is web Services Security (WS-Security). This standard defines application-to-application security that can pass sensitive portions of the message through intermediate applications without decrypting the message. Message encryption between sender and receiver provide a firm basis for message authenticity and non-repudiation.

The security subcomponents include identity management, role based access control, encryption, public key infrastructure, digital signatures, and threat protection. Additionally, the security subsystem configuration supports SSO capabilities and data auditability to enable a recorded history of actions performed.

Role-Based Application Access Control Through Medicaid Enterprise User Provisioning System (MEUPS)

Applications process and deliver sensitive data, such as Medicaid clients' PHI and PII.

Approach

Role-based access control operates within the applications and subsystems of Colorado interChange. The MEUPS establishes a security profile for each user that determines which applications and functions the user is authorized to access. We use a defined approval process to grant access privileges, and review them regularly to help promote proper availability and confidentiality.

Benefit of this Approach

HP has extensive experience in implementing role-based access control for applications used by Colorado interChange. Our combination of experience, integrated access control technologies, and standards-based policies and procedures are unmatched by competitors (UID: 1195 – Technical controls).

Managing application access is a critical aspect of risk management and security. HP manages the access and exchange of information through integrated security across the MMIS applications and portals to provide, control, and manage role-based access and authentication to the proper applications, panels, and data.

Our formal user provisioning and de-provisioning procedure grants and revokes access to information systems and services. We assign user with need-to-know criteria to prevent unauthorized access to, or disclosure of, sensitive information. Policies and procedures define a process for assigning, reviewing, and revoking access privileges. We also inform users of policies governing acceptable use of applications and any sensitive information.

We use role-based access control protocols to restrict access to sensitive information in applications. This approach restricts access to applications such as Colorado interChange and the HP Healthcare Provider Portal. Security profiles will be established for HP employees, Department users, and stakeholders who have Department-authorized access to the various components of Colorado interChange.

User Administration Module (Unique ID 1204)

The Colorado interChange solution provides SSO for authorized MMIS users to access integrated enterprise applications by Microsoft Active Directory Federation Services. We have a comprehensive security solution that provides centralized identity management. HP provides a single point of access for authorized system users. Centralized user authentication and authorization, as well as de-provisioning a terminated user, is accomplished with a set of interoperable tools.

The solution also allows for user self-provisioning. Based on user type, accounts can be created through access to a web page, an internal link, or PIN information sent through the mail with a provider ID. Providers are automatically given the appropriate authorizations based on their enrollment information. Internal fiscal agent or State staff users can request access to MMIS applications as needed. Requests route through preconfigured workflows of approvers who approve or deny the requests for authorizations. The authorization request process is managed using emails sent to the series of approvers. Status emails also are sent to everyone involved with the request.



Security solution includes workflow user provisioning to allow efficient access and assignment of roles to users within the solution. User provisioning and management is a critical part of the security process. Not only should the process have controls and workflow, but the process must allow for the detailed user management necessary so that the proper controls are in place for system access. This also means users do not have to wait days for access to timely information for self-management. This means that the emphasis is placed on policy and policy monitoring, not the work to do it. This component of the solution allows for quick user auditing and review of user management and access.

We provide additional detail on the security access request process in RESPONSE 38g.

Because the security provisioning is worked and tracked electronically, we can easily report an audit of the applications in the environments to which users have access. While other vendors

attempt to track such information on manual tallies or through spreadsheets, our solution provides an auditing report ability linked directly to the actions taken through the provisioning.

Easy-to-Use Module (Unique ID 1205)



Designated administrators can add users and groups at the site, library, data, and task level in interChange, based on their defined work role or work group requirements. User profiles will control what information is accessible to individuals who are authorized to have access to Colorado interChange and the capability approved such as: "inquiry only", "update", or "add" capability.

Using MEUPS, the administrator can assign a preset user role or create customized profiles to enable or restrict access to specific parts of the application(s).

State and fiscal agent staff user IDs are grouped based on organizations and departments. Many organizations can be defined within the solution. Each organization must have one or more departments. Each internal user is assigned to one organization and one department. These assigned groups are the basis for the authorization approval workflows that are processed when a user initiates an authorization request. Owners of these groups can be given the authority to manage configuration of the group, add users to the group, and terminate users in the group

Additionally, the Provider Portal restricts providers' access to member information from a defined set of constraints in the Colorado interChange. A provider can designate "delegates" (such as billing agents) to have access to the Provider Portal through a unique log on. The provider can then assign one or more functions - made up of one or more security rights – to each delegate. For example, a function for claims inquiry will contain the security rights needed to perform that function. Likewise, a function for claim submission would allow a delegate to submit claims. Administrators or providers (as the State permits) can be allowed to define security functions available to delegates in the provider portal, as seen in the following figure.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

The provider controls access to functions for each delegate. A delegate representing multiple providers can have different security access for each provider represented.

Support for Role-Based and Group-Based Security at Individual Data Field Level (Unique ID 1207)

As previously noted, the Colorado interChange supports role-based and group-based security at the site, library, data, and task level. This helps to confirm that users have the correct information available to perform their work role at the appropriate time.

Suppressing results returned is configurable in the Colorado interChange to a certain extent; required system enhancement will depend on the business rules for the data to be suppressed. For example, the system allows the suppression of a search result's field based on a user's security role; more complex requirements to suppress search results based on a user's work location would require an enhancement—for example, enabling an eligibility clerk in a specific county to view information for clients residing outside her county.

Secure Access to External Portals (Unique ID 1764)

Our security solution will support integration to BIDM through SSO using a standard SAML token. Authorized users can access BIDM through the Healthcare Portal.

7.6 – Security and Confidentiality Requirements	In Production? YES/NO
Description Addresses Requirements (Provide the range as applicable): 1206, 1208	NO

Privacy and Litigation Controls (Unique ID 1206)

Colorado interChange access is configurable to accommodate needs such as user restrictions and legal holds. Role-base security, assigned per Department specifications, helps verify that the system, by default, will not provide access to this information unless specific authorization is given. This means access to PHI/PII or other sensitive information is automatically not provided, but can be incrementally added based on the Department's discretion. This also means that data classification is included as a component of data exports to allow for the default exclusion of certain specific information.

Screens for Security Personnel (Unique ID 1208)

Please see RESPONSE 49 for detail on this optional requirement.

RESPONSE 38f

7.7 – Audit Requirements	In Production? YES/NO
Description Addresses Requirements (Provide the range as applicable): 1209-1220	YES

HP's audit trails maintain data and system integrity while protecting data accuracy and preserving an accurate historical record of changes made in the system. HP monitors actions, authorized users, and system performance internally while our change management process maintains the overall integrity of a project.

When political pressures, budget mandates, or legal action require complex, time-critical changes impacting multiple moving parts, HP can assist the Department with our experienced, knowledgeable staff members who understand the technical intricacies of the Colorado interChange MMIS and the sensitive nature of those impacted by the Medicaid program. We have a track record of stepping up to any challenge with a “do-what-it-takes” attitude. We have a defined process and automated tools to manage change.

Appropriate audit trails are automatically created for adds, deletions, and changes to the following files:

- Provider records
- Client eligibility
- Claims
- Reference data
- Web access
- Encounters
- Electronic images

The audit trails are readily available to authorized users. Audit information can be filtered by fields (columns) or system date ranges and can display results for only the selected record or for the records in the parent panel. Electronic document management system (EDMS) reports show the number of documents that came into the system and were exported from the system by document type and active batches in the system.

Change Management (Unique ID 1209)

The Colorado interChange will include audit trail functionality for tables and can be configured, as needed, at the database table level regardless of whether the changes are coming from the user interface or in batch. Under the change management plan, we provide the ability to review

changes made to fields in the system. We will adhere to the deliverable submission, review, and approval as described and approved by the Department within the change management plan.

An effective change management plan addresses multiple types of change and is imperative to mitigating scope, schedule, cost, and risks. Success for the COMMIT project depends on the clear definition and management of project scope, cost, schedule, quality, and configuration items. HP's change management plan is a subsidiary plan to our project management plan.

Provider Records (Unique ID 1210)

The Colorado interChange will provide full audit trail functions on the provider database tables. The audit trail is available online for each tab within the provider subsystem and shows the additions and changes. This includes modifications to status and limitations or restrictions. The following figure shows the audit trails related to the provider application.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

For each tab, the user specifies the fields to include in the audit trail and start and end dates. The user then clicks on search and receives the search results as seen in the following figure.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**



The user can now see the information that was on file and the date, time, and ID of the individual user or system ID that modified or created the record.

Written communication with the provider is stored in OnDemand and available for viewing. This includes letters sent to and received from providers, and the results of verifications with third-party sources regarding credentialing and third-party validation.

Eligibility (Unique ID 1211)

The Colorado interChange will provide auditing functions that capture information such as date, time, user ID, and data from the record when inserts, updates, or deletions occur on a database table. Regardless of source, such as UI or batch, the audit data will be captured. Additional auditing is established case by case.

We will retain eligibility data, as seen highlighted in the following figure, in the Colorado interChange. The previous IDs will provide a listing of the previous IDs for a client. Additionally,

the link history feature enables authorized users to link multiple IDs for a given client. Audit functions verify that the changes to data are logged by date and user information. The EDMS solution stores communication associated with a client.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**



Claim Records (Unique IDs 1212, 1214)

(1212) Colorado interChange maintains a complete audit trail for each claim record. Error codes encountered by the claim are captured and displayed on either the claim level error screen or the detail error screen. As shown in the following figure, (1214) the interChange solution captures: the date/time stamp of each action taken, whether performed automatically or manually; the system or user ID performing the action; and the status of the error code. User-applied changes such as data corrections are captured in audit trails along with the ID of the user performing the update.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

The Colorado interChange MMIS will use location codes as shown below to monitor and control the movement of each claim through adjudication. The date and time the claim enters a location code is captured and available online for review as seen in the following figure.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

The rules used to process each claim are captured and displayed on the decision rules screen shown in the following figure. This screen shows every rule, the order of the application of the rules, and the level to which the rule was applied (header or specific detail number).

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

Clicking on a particular rule will open a new window displaying the business rule editor with the actual rule highlighted. This enables complete traceability from the claim to the applied rule.

Adjustments (Unique IDs 1213)

Each claim receives a unique internal control number (ICN) for tracking purposes and future reference. The original submission of the claim is linked to all subsequent adjustments including partial and system-generated adjustments. As the following figure details, the Colorado interChange will include a panel that displays prior and subsequent versions of a claim.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

Users can click on the ICN of the adjustment claim and the claim will open in a separate window for viewing, allowing users to see the original claim and the adjustment claim side by side.

Interface Data Modification (Unique ID 1215)

The Colorado interChange will have auditing features that can be configured as required at the database table level regardless of whether the changes are coming from the UI or batch. When the interface feed updates an interChange database table, an audit record is created for those tables that have auditing configured.

EDMS (Unique ID 1216)

The OnDemand EDMS will maintain an audit trail to identify the date a document was placed in the system along with actions taken on the document or attachment by user ID.

Using Audit Trails (Unique ID 1217,1220)

(1217, 1220) As the following figure details, the Colorado interChange UI will enable the users to view audit trail records through the audit panels.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

The Colorado interChange will track updates to data through batch, real-time external interfaces, or web panels, allowing a complete audit and reporting process. The audit trail records the action (insert, update, or delete), date of the change, the source of the change (electronic file or staff ID making the change), and what information changed because of the update.

System Access (Unique ID 1218)

The Colorado interChange will track changes made by an individual user through audit trails. To monitor viewing, HP uses Oracle AuditVault to provide fully configurable field-level auditing of records viewed by users. Access into the computer systems and applications will require an ID and an associated password. At the network level, we use the ID and password to identify the users and authenticate whether the user has access to a personal computer, a network, or an application. At the application level, the ID and password identify the user, authenticate what data the user can access, and assess if the user can only view the data or if the user can change or delete the data.

Provider and Client Websites (Unique ID 1219)

The Healthcare Provider and Client portals support the logging, tracking, and auditing of web access for any client-data or provider-data queries. The data is captured and passed to the Colorado interChange MMIS. For example, the results of a web customer eligibility inquiry are passed to and viewable in the Colorado interChange Enrollment Verification Panel as seen in the following figure.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

Rather than capturing only verification inquiries that meet specific criteria, the underlying table captures each inquiry. Users have immediate, online access to review inquiries by provider ID or client ID. Drill-down capability allows the user to view details of the inquiry, including dates of service the provider seeks. A verification number is assigned and the exact results returned to the provider are stored in the table.

RESPONSE 38g

7.8 – Compliance with Federal Standards Requirements	In Production? YES/NO
Description Addresses Requirements (Provide the range as applicable): 1196, 1200, 1221-1233	YES

HP continues in its role as a trailblazer in MMIS developments—something we started more than 40 years ago. We will implement an advanced MMIS for the Department, meeting federal compliance standards.



HP's understanding of the work requested began with a thorough review of the Department's objectives for the scope of work by a group of our experienced specialists who draw on our HP Best Practice Repository and implementation experience. We built our repository of proven practices from lessons learned and practices refined through our numerous implementations.

The repository, as seen in the following figures, is one way we verify that proven processes and practices are repeated for successful implementations.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**



**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

We divide the Repository into categories. Users can drill down to documents that have been through review and updates to retrieve the attachment for the topic for which they are working, such as roles and responsibilities to assign for a successful certification process.

The Department's objectives are similar to those of our other customers:

- Transition to operations without disruption to the providers or clients
- Achieve certification retroactive to day one; comply with HIPAA requirements
- Provide timely deployment of provider-facing components
- Improve efficiency
- Minimize risk
- Meet federal standards

HP and our proposed Colorado interChange Medicaid Enterprise system fit the Department's requirements and federal standards, as outlined in the remainder of this response and in the links supplied to other standards we address in other responses as appropriate.

System Meets Requirements (Unique ID 1196)

During the Organizational Readiness and Training Phase, we will demonstrate that the Colorado interChange business and functional areas are operational and ready for implementation and rollout. This includes meeting federal and State architectural, technical, security, and privacy requirements. Using these requirements as the foundation for our construction and adding the Department's requirements during the Development Phase validates HP will meet the standards at implementation.

During system verification and validation, HP documents that infrastructure, software, communication, and security requirements have been implemented according to defined and documented security and functional requirements. We focus on actions supporting increased confidence in the correct implementation and operation of the control. An essential part of the control includes specific capabilities and documentation to demonstrate that the control meets its required function or purpose. Auditors use this documentation to analyze and test the functional capability of the control.

Secure Sign-On (Unique ID 1200)



Protection of Medicaid data is of utmost importance to every state—and to HP. The need to wrap the data in a security blanket comes with challenges when allowing access, as needed, to those users authorized to view or edit the data. Security around the MMIS and peripheral systems has become a full-time job, sometimes at the cost of delaying access in the interest of “getting it right.” interChange Security is the value-added solution from HP to verify access is granted correctly and promptly for each user to each program or application needed after meeting the applicable approvals.

We offer a comprehensive security solution that provides centralized identity management. HP will provide a single point of access for authorized system users. HP accomplishes centralized user authentication and authorization and de-provisioning of terminated or inactive users with a set of interoperable and automated processes.

Historically, users were burdened with separate user names and passwords for separate systems based on their job duties and level of responsibility. Provisioning those names and passwords could take days and require separate forms for separate functions. Our solution uses Active Directory to achieve the following:

- Single log on and authentication
- Self-service provisioning
- Delegation
- Role management and help desk
- Password management, including self-service password reset capabilities
- Hierarchical security group and permissions structure



Instead of having an assortment of forms for requests, we will create a consistent method for requesting access to applications and network resources. The solution manages user access through automating the request and approval that replaces the existing manual and paper-driven processes.

Because of the simplified logon process, single sign-on will yield positive gains in worker time and efficiency. Workers will log on to their workstations and automatically gain access to the applications they have been authorized to use through the landing page.

Because of the success of this proposed interChange solution with the Kentucky Medicaid program, the commonwealth implemented it across its entire commonwealth system.

Commonwealth employees in Kentucky estimated gains of two minutes per day per worker—a substantial savings when multiplied by 2,785 workers for 252 working days per year—achieving a savings of 1,403,640 minutes annually. This is just in logon time alone. We achieved further savings by reducing help desk staff members, lowered paper costs by eliminating forms, and reduced downtime for staff members waiting for password resets.

HP can bring these same results to the COMMIT project. interChange Security will deliver significant return on investment to the Department. The security foundation we provide brings system access to the forefront of technological advances.

How It Works

HP's Active Directory security solution is interoperable with other user management systems and can be connected to the Department's user repository to provide single sign-on to applications other than the Colorado interChange MMIS:

- **Single sign-on and authentication**—The solution provides single sign-on for Colorado interChange users to access integrated enterprise applications by Microsoft Active Directory Federation Services. Authenticated credentials and roles are passed through standard SAML tokens to the receiving application for use as application-specific authorizations. Colorado interChange users can access applications through links on the landing page. This is the starting point for Medicaid activities through the web. Activity through the landing page is logged and reportable. Routing users through the logon page before initial application access also handles direct access to individual applications using “deep links.”
- **User self-provisioning**—The interChange solution allows for user self-provisioning. Based on user type, accounts can be created through access to a webpage, an internal link, or PIN information sent through the mail with a provider ID. Providers are automatically given the appropriate authorizations based on their enrollment information. Internal fiscal agent or State staff users can request access to Colorado interChange applications as needed. Requests are routed through preconfigured workflows of approvers who approve or deny the requests for authorizations. The authorization request process is managed using emails sent to the series of approvers. Status emails also are sent to everyone involved with the request.
- **Delegation**—Providers can allow administrative office staff members or contracted billing agents to access Colorado interChange functions for them while maintaining a separate set of authentication, authorization, and security audit information. Each administrative staff member and contracted billing agent will have a separate logon ID. Through interChange Security, providers can delegate selected authorizations to these accounts based on the account owner's roles within the provider's business processes. Those links are maintained, even across providers, while having an individual identity for each delegated user.

- **Role management and help desk**—The Colorado interChange provides a help desk application to manage the aspects of configuration: users, applications, and roles with corresponding reporting features for each. The help desk is the central control center for daily operations. The call center staff will be given basic access to the help desk (not administrative access) to manage user calls related to typical security issues.
- **Password management**—The Colorado interChange allows for self-service password resets using a link on the security logon page. When the user clicks the link, the system generates an email to the user's registered email address. A link takes the user to a page with a preconfigured security question. The user must answer the question successfully to reset the password.
- **Hierarchal structure**—State and fiscal agent staff user IDs are grouped by organizations and departments. Many organizations can be defined within the solution. Each organization must have one or more departments. Each internal user is assigned to one organization and one department. These assigned groups are the basis for the authorization approval workflows that are processed when an authorization request is initiated by a user. Owners of these groups can be given the authority to manage configuration of the group, add users to the group, and terminate users in the group.

User Provisioning



Exceeding the basic security management requirements, the Colorado interChange Security solution will include workflow user provisioning to allow efficient access and assignment of roles to users within the solution. User provisioning and management is a critical part of the security process.

The process has controls and workflow and must enable the detailed user management necessary so the proper controls are in place for system access. This also means users do not have to wait days for access and can obtain the information they need promptly to self-manage. This means that emphasis is placed on policy and policy monitoring, not the work to do it. This component of the Colorado interChange allows for quick user auditing and review of user management and access.

The following figure illustrates a user requesting security access to specific applications within specific environments.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**



Security requests are routed through preconfigured workflows of approvers who approve or deny the requests for authorizations. The authorization request process is managed using emails sent to the series of approvers. Additionally, status emails are sent to everyone involved with the request.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**



The following figure shows the screen that a manager will use to authorize the security request. Managing the security requests through this online controlled set of defined workflows provides the oversight and efficiency required of an enterprise-wide MMIS offering.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

Because we work and track the security provisioning electronically, we can easily report an audit of which users have access to specific applications in the environments. Our solution provides auditing report ability linked directly to the actions taken through the provisioning system.

Certification (Unique ID 1221)

HP has unparalleled experience certifying MMISs under the latest certification rules. We were the first fiscal agent in the nation to gain certification using the new CMS MECT checklists. HP remains current on the State Medicaid Manual (SMM) Part 11 and the Code of Federal Regulations (CFR) as applied to Medicaid and Medicare. As CMS makes changes or highlights best practices, HP reviews and implements them as applicable. HP leaders on each account keep abreast of the changes, discuss them internally with peers, and proactively discuss SMM and CFR changes, and recommend actions to the State as needed.



HP provides customers with federally certified business solutions based on interoperability and configurability with integrated business process functions. We have certified a record number of MMISs since 2002—more than all other vendors collectively have achieved in the same time frame.

The Department can be confident about achieving certification as HP will apply lessons learned from our 12 previous CMS certifications to help the Department prepare for the certification process.

Each of our interChange implementations, before and after the adoption of the new MECT checklist, received the official seal of approval from CMS. The only exception is with Kentucky, where we certified on day 14.

Although we have many tools and proven practices related to the certification process, the reason for our successful certifications is the solid system design of the interChange solution. Our system exceeds the requirements for CMS certification in many areas. For example, in Wisconsin's certification approval letter, CMS called out six of our specific business and technical processes as Industry Best Practices (IBPs) over and above their existing defined IBPs. As we detail in RESPONSE 14, CMS commented positively on the design and efficiency of the system, and that the business process coordination across business functional areas is geared toward cost savings and continuous improvements.

We also have continued to receive positive comments for our efforts in Massachusetts, Oregon, and Georgia. We will bring this industry-leading knowledge and experience to the Department's COMMIT project. The following table summarizes the certification benefits gained by choosing HP to design, develop, and implement the Colorado interChange MMIS.

Certification Benefits

Features of the HP Solution	Benefits to the Department
Successful track record of certifications for the last 10 years	Offers the Department a high level of confidence and likelihood that the Colorado interChange will achieve certification
Ability to certify the Department retroactive back to day one of operations	The Department will maximize federal funding by meeting the conditions for certification back to day one.
Ability to certify the Department quickly with no findings	Speed to certification reduces customer investment

By selecting HP to implement the Colorado interChange and support the Department's federal certification activities, the Department will have a reliable, skilled team with recent experience in successful MMIS CMS certifications.

Please see RESPONSE 1 of this proposal for a full explanation of why HP is so successful in gaining certification. Our processes and procedures are outlined in depth in that section.

ACA Provider Screening Rule (Unique ID 1222)

HP has read Appendix G, Section G6.0 to fully understand the Department's current situation, plans for the future, and the role of the new fiscal agent in implementing the provisions of the Patient Protection and Affordable Care Act (ACA) Section 6401 specifying procedures under which enrollment and screening is conducted for providers.

Item 4, page 2 of the letter to CMS fully explains what the Department expects from its new fiscal agent:

“The Department will implement the tools and processes necessary to fully comply with the Rules as a first priority of the replacement MMIS and fiscal agent contract. For example, the successful responder to the RFP for the replacement MMIS is required to provide a tool for online provider enrollment (OPE) by July 2014 and to propose a plan to complete provider re-enrollment by March 2016 as required by the Rules.”



HP understands this clearly and will fully engage the Department immediately after contract execution and begin work to verify the commitment to CMS is upheld. To meet the ACA Provider Screening Rule, as part of the provider enrollment process, HP will check sanctions, licensure, and conduct screening of potential Colorado Medical Assistance providers.

We use LexisNexis to meet the requirements of Rule 6028 of the Affordable Care Act (ACA) for provider credentialing and background checks. The HP staff pulls information from a large database, provided by LexisNexis, of public and proprietary records to give a detailed view of individuals or businesses and their history. This service aids in the investigation process by quickly identifying fraud and other incidents within the last five years that involve owners, indirect owners, and managing employees.

LexisNexis compiles reports on companies and individuals associated with a tax ID or Social Security number. These reports can include such information as civil judgments and liens, bankruptcies, court and regulatory rulings, negative news and felony charges. LexisNexis also can validate and authenticate the identification credentials of potential providers.

Files regularly submitted to LexisNexis contain provider information and the names of individuals and entities listed on the disclosure forms, including managing allies and individuals with more than a State-defined percentage interest in the business. We will work with the Department to define processes for providers with negative information identified during screening and determine the frequency of file submissions to LexisNexis.

We detail the Online Provider Enrollment solution in RESPONSE 39b.

Reporting Data and Documentation (Unique ID 1223)



HP has been at the forefront of the reporting revolution within the Medicaid industry. The right data collection, reporting, and analysis can help the Department improve operations and better manage healthcare program dollars. Through decades of experience generating and providing these reports from several state implementations, HP has a strong breadth of knowledge of what is needed to create and deliver federal reports. To promote the Department's compliance with federal reporting, HP will work to create the extract files that contain the data attributes the business intelligence data management (BIDM) vendor needs to meet their requirement. We will oversee the transfer of methodological documentation for the federal reporting from the BIDM

vendor who has the responsibility for creating the reports. The documentation will be stored within the content management solution of the Colorado interChange MMIS to meet the requirement.

The data transfer from the Colorado interChange MMIS to the BIDM vendor will be tightly managed by the interChange Connections module for interoperability. This MMIS module provides the data transfer reliability required for making sure the MMIS source data is transferred to BIDM. The detailed transactional data will provide the necessary information to the BIDM to generate the following reports to meet CMS federal and State reporting requirements:

- **CMS-372**—Annual Report on Home and Community-Based Services Waivers
- **CMS-372S**—Annual Report on Home and Community-Based Services Waivers and Supporting Regulations
- **CMS-416**—Annual EPSDT Participation Report
- **CMS-37**—Medicaid Program Budget Report
- **CMS-64**—Quarterly Expense Report
- **CMS-21**—Quarterly CHIP Expenditure Report
- **CMS-21B**—Quarterly CHIP Program Budget Report
- **PERM**—Payment Error Rate Measurement

The data transfer from the Colorado interChange MMIS to the BIDM solution to support the federal reporting requirements will be tightly managed by the interChange Connections module. The Connections module is powered by Microsoft BizTalk for ESB interoperability. This MMIS module provides the data transfer traceability and reliability required for making sure the MMIS source data is transferred to the BIDM.

Data for T-MSIS Files (Unique ID 1224)

The Colorado interChange MMIS provides the claims data for the CMS-required Transformed Medical Statistical Information System (T-MSIS) files. These files include data for client eligibility, inpatient claim activity, long-term care claim activity, other claim, and pharmacy claim activity. The MSIS summary process produces these files quarterly. Data is delivered to the BIDM contractor through electronic file exchange. We will update the MSIS files per the T-MSIS files specifications and data dictionary document.

Because federally mandated requirements affect each of the states we support, we collaborate to share ideas and solutions. With each of our Medicaid accounts represented, the HP T-MSIS Leveraging Work group provides an online forum, along with routine meetings, for team members to pose questions, seek advice, and provide ideas for an effective transition. At these

meetings, our account leaders discuss implementing new federal mandates and collaborate on how best to implement the mandates, sharing ideas and potential issues.

Data for CMS-372 and CMS-372S Annual Reports (Unique ID 1225)

HP will provide data for the CMS 372 and CMS 372S annual reports, generated on the schedule and in the format specified, with format and frequency adjustable as requirements change. This report is designed to determine program participation, expenditures, services, paid and billed amounts, eligibles, unduplicated client counts, total cost of care by date of service, and expenditures for parallel populations.

Data for EPSDT Reports (Unique ID 1226)

HP will provide data to generate standard EPSDT reports to meet federal and State reporting requirements.

Data for CMS-416 EPSDT Reports (Unique ID 1227)

HP will provide data for the CMS 416—Annual EPSDT Participation Report. We will accurately capture and provide this data to the BIDM vendor within the specified time frame.

PERM Data (Unique ID 1228)

HP has established procedures and protocols for extracting data to support the National Payment Error Rate Measurement (PERM) reviews. We will accurately capture and provide this data to the BIDM vendor within the specified time frame.

Data for Financial Reporting (Unique ID 1229)

HP will capture and provide to the BIDM the data required for the BIDM to produce financial reporting based on Department-defined criteria and produce quarterly estimates and expenditure reports for federal CMS-37, CMS-64, CMS-21, and CMS-21b.

X12 Transactions (Unique ID 1230)

The Colorado interChange will provide payment transactions through the X12N 820 format. Enrollment transactions are in X12N 834 format. HP's interChange Connections EDI solution is a readily available channel for exchanging HIPAA transactions. An important aspect of EDI is verifying that incoming and outgoing X12 transactions meet the HIPAA standards. interChange Connections validates X12 transactions for HIPAA compliance as they are received and before they are sent to our trading partners. The batch and real-time submission mechanism can validate and accept or reject X12 transactions and respond with appropriate HIPAA acknowledgment transactions such as 999 and TA1.

interChange Connections offers flexible mapping that is fully compatible with each of the components of HP's EDI solution, offering the acceptance of various formats and transactions. HP's EDI interChange Connections provides the ability to translate a message into a format that is understandable to the service that will receive it.

ADA and WCAG Compliance (Unique ID 1231)

The Healthcare Portal we will deliver to the Department is a secure and compliant platform that adheres to HIPAA, National Council for Prescription Drug Programs (NCPDP) requirements, and ADA Section 508.

Our portal also meets Web Content Accessibility Guidelines (WCAG) 2.0 as outlined in the following table.

WCAG

WCAG Guidelines	HP Solution
1.1 Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, Braille, speech, symbols or simpler language.	We have hover-text for each item on the page and alt-text icons for additional instructions. The ability to increase or decrease text size can be made available.
1.2 Provide alternatives for time-based media.	Our time-based function is related to inactivity timeout for security reasons. During the ADA Section 508 compliancy initiative, we added an interim step to prompt users that their session will time out because of inactivity. The amount of time before auto-log off is customer-configurable. Also, within the prompt, users can request additional time for their sessions, essentially resetting the timer.
1.3 Create content that can be presented in different ways (for example simpler layout) without losing information or structure.	The portal has a simple structure. The pages are consistent in their design and layout.
1.4 Make it easier for users to see and hear content including separating foreground from background.	Our feature with a foreground and background scenario is pop-up messages in response to user actions. These display in the foreground and a screen reader would automatically pick them up.
2.1 Make all functionality available from a keyboard.	The user can navigate to pages, panels, or fields using the TAB key to go forward and Shift-TAB to go backward.
2.2 Provide users enough time to read and use content.	See 1.2
2.3 Do not design content in a way that is known to cause seizures.	As part of ADA Section 508, we confirm we have no flashing or flickering items on the screen.
2.4 Provide ways to help users navigate, find content, and determine where they are.	The portal uses breadcrumb, tabular menu, and help tools.

WCAG Guidelines	HP Solution
3.1 Make text content readable and understandable.	Text in the portal is configurable. Default text is geared toward a sixth-grade reading level.
3.2 Make Web pages appear and operate in predictable ways.	The portal has a consistent look and feel throughout.
3.3 Help users avoid and correct mistakes.	The portal has predictive search lists where the user can start typing the first few characters and a related list will display an option allowing them to choose from drop-down lists, calendar icons where the user can select a date, and error messages when items are entered incorrectly.
4.1 Maximize compatibility with current and future user agents, including assistive technologies.	The pages were tested using a screen reader during the ADA Section 508 compliancy testing in 2010 and again in Release 4.2 in 2012.

Health Literacy (Unique ID 1232)

When producing client and provider communications, HP will verify that the communications contain verbiage that meets the health literacy level established by the National Institute for Health (NIH) and state guidelines.

HP embraces the NIH philosophy of improving health outcomes by communicating clearly regarding health issues. The type of communication commonly associated with health literacy that would apply to HP publications in the COMMIT project include the following:

- Patient and physician communication
- Health information publications and other resources
- Informed consent documents
- Responding to medical and insurance forms
- Training

“[Health Literacy is:] The degree to which individuals have the capacity to obtain, process and understand basic health information and services needed to make appropriate health decisions.”

—Healthy People 2010

Our documents, letters, and other communications follow the toolkits and guidelines available from NIH.

Reading Literacy (Unique ID 1233)

As required by the RFP and federal regulations, HP will use a sixth-grade reading level when publishing client and provider material for the Colorado Medicaid program.

RESPONSE 38h

7.9 – Disaster Recovery and Business Continuity Requirements	In Production? YES/NO
Description Addresses Requirements (Provide the range as applicable): 1023, 1234	YES

HP invests heavily in the design and preparation for business continuity and disaster recovery. Reliability, dependability, availability, and serviceability are a top priority for HP within the healthcare industry. As the unsurpassed leader in healthcare claims administration, and drawing on more than 45 years of healthcare industry experience, HP has established policies and procedures to manage various disaster recovery scenarios.



HP's disaster recovery and business continuity experience and lessons learned enables us to prepare for and respond to disasters while continuing operations to support the COMMIT project.

We achieve both disaster recovery and business continuity through two critical aspects:

- **Systems**—To be restored to operational state with the data, hardware and applications components
- **People**—To be able to work on the system so that the services could continue

Unique Aspects of Healthcare and Medicaid Programs



Our approach provides a sound solution to the business and operations while managing costs. It is built on flexibility, geographic diversity, and world-class infrastructure. HP will use the Colorado Disaster Recovery site to support the COMMIT project.

HP can deliver services to clients as soon as possible after a declared disaster, to restore particularly vital functions, such as:

- Benefits and eligibility verification
- Inbound claims traffic and processing
- Payments to providers
- Outbound remittance advice and explanation of benefits traffic

Because Medicaid programs cover some of the most at-risk clients in society, it is critical to quickly restore services from social, economic and political perspectives:

- Minimization of downtime, outages, and interruptions provides virtually uninterrupted delivery of healthcare services to Medicaid clients.

- Higher participation rates from the provider community when claims are processed in a timely and accurate way through minimized disruption.

Unique Aspects of HP in Healthcare and Medicaid Areas

HP has more than four decades experience in developing and managing disaster recovery and business continuity services. As evidenced in the figure below, HP is a recognized leader in offering global business continuity and disaster recovery. Real-world experiences allow us to continuously enhance our MMIS disaster recovery and business continuity methodology. These improvements enhance our ability to limit the scope and duration of effects from disaster events.

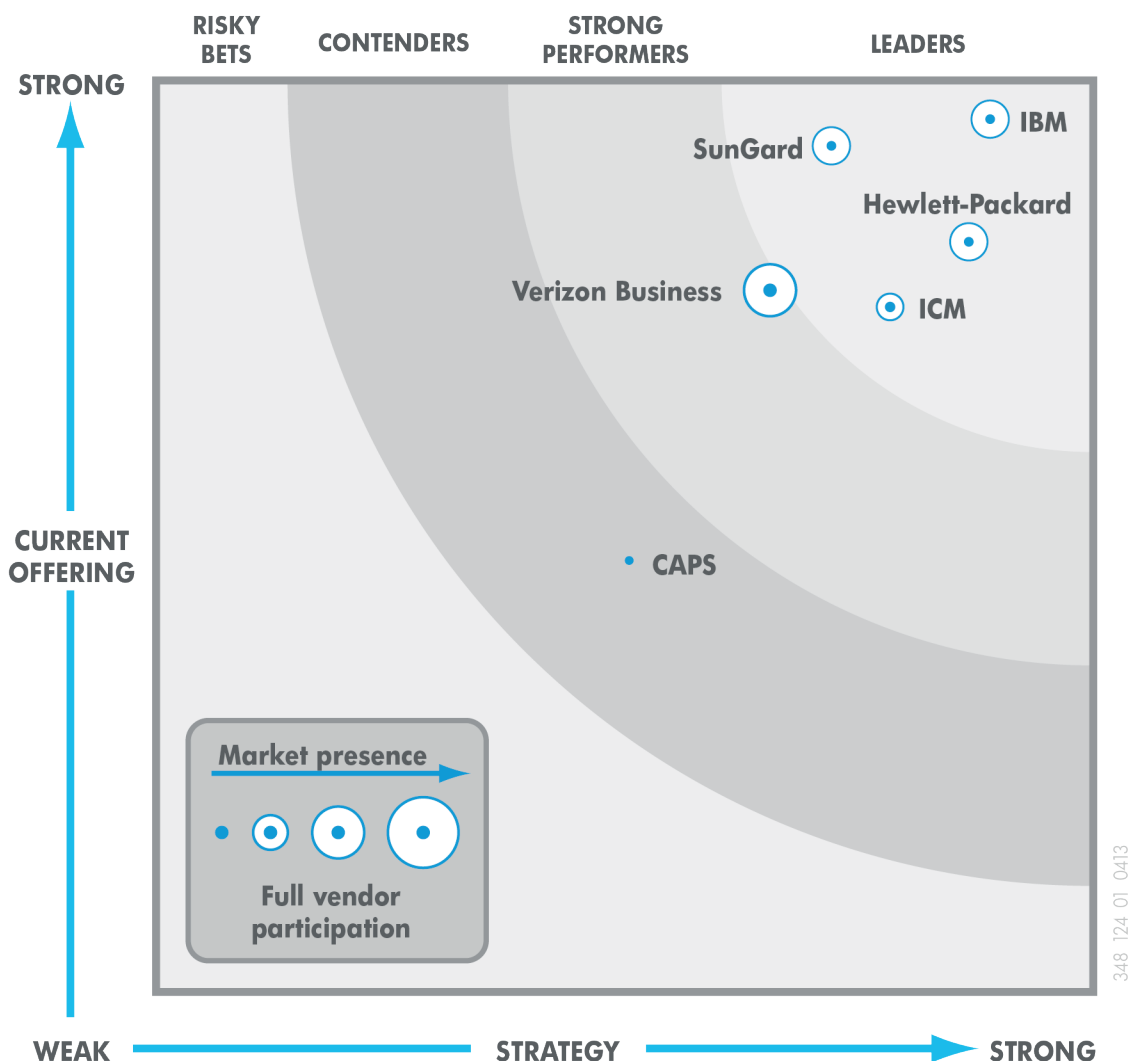
HP is one of only two vendors offering global business continuity and recovery services. We have more than 5,000 disaster recovery and business continuity customers worldwide.

We have technology expertise across multiple platforms from major suppliers, coupled with multivendor expertise in designing and implementing disaster recovery and business continuity solutions for HP, IBM, Oracle, Dell, EMC, VMware, and other environments. This combined experience allows us to meet and exceed the Department's requirements in preparation for, and in response to, disaster events.

In June 9, 2010, "*The Forrester Wave™: Disaster Recovery Services Providers, Q2 2010*" reported HP as a "strong leader". Forrester's assessment used their 64-criteria evaluation of disaster recovery services providers. HP is proud that Forrester identified us as one of the leaders and best-in-class core disaster recovery service providers. The following figure demonstrates our capabilities as a disaster recovery service leader in the industry.

Forrester Wave Disaster Recovery Providers

Forrester Wave™: Disaster Recovery Service Providers, Q2 '10



HP provides proven strategies, services, and technologies to reduce the Department's exposure and vulnerabilities. This helps protect critical operations against downtime threats, and ease recovery in case an unforeseeable catastrophe does strike.

HP's Experience in Healthcare and Medicaid Disaster Recovery

Our disaster recovery plan encompasses processes, methodologies, and procedures. These describe the roles, responsibilities and actions necessary to resume COMMIT operations if a disaster event occurs. We have proven success in assisting Medicaid customers around the country as they faced weather challenges. Our 2010 assistance to the State of Oklahoma account during a natural disaster is detailed below.

Torrential Rains Don't Dampen Customer Service

Oklahoma City, Oklahoma—When treacherous weather threatened the Oklahoma Health Care Authority's ability to conduct business, the HP Oklahoma Title XIX account team stepped in to assist its client to continue serving those in need of Medicaid services throughout the state.

The Oklahoma Health Care Authority (OHCA) is the primary entity in the state of Oklahoma charged with controlling costs of state-purchased health care. HP processes health care provider claims, operates call centers, produces reports, generates letters, and completes payments for about 28,000 providers and more than 700,000 Medicaid recipients using HP's MMIS on behalf of the OHCA.

In early summer of 2010, a series of major storms struck the Oklahoma City area, causing destruction that forced the OHCA to abandon its facility. Motorists struggled to navigate flooded streets in Oklahoma City after 11 inches of rain fell in a five-hour period. The torrential rainfall eventually caused the customer's roof to collapse as flood waters overtook the surrounding streets. With the first floor of the building flooded and the second floor heavily damaged, many OHCA employees found themselves with no workspace or office equipment. That's when their HP colleagues stepped in to lend a helping hand.

HP employees volunteered to stay late and help, rounding up spare office equipment and creating makeshift work spaces to accommodate as many displaced OHCA employees as possible.



348_072_04_0513

Business Continuity—Real-World Examples

Examples on how we have previously addressed business continuity requirements of our Medicaid accounts are summarized below.

- **Call Center Flooding**—In 2011, flooding occurred throughout the state of Rhode Island. The building housing Medicaid operations was completely under water. Within 24 hours, calls were routed to alternate inbound trunks. We set up an announcement to advise callers of the state of the emergency and when we expected operations to be restored. Within another 24 hours, we had agents in place to answer calls, restored connectivity to the network, and had the call center operational as usual.
- **Call Center Relocation**—Phase two of supporting the Rhode Island disaster involved moving agents into a temporary space where IP-soft telephone and IP-agent software was used to enable the agents to continue working. This capability is available for any new site and with preparation can be used immediately for a short-term or long-term outage.
- **Increased call volumes**—Call centers in California and Kansas answered calls from the states of Kentucky, Florida, Oklahoma and Connecticut in the past several years when call volumes increased unexpectedly. Changes to network routing allow the agents to access systems in the other states. It is an HP standard to cross-train agents in other states who are caring for Medicaid providers or clients, allowing HP to bring agents up-to-speed quickly on a specific state's systems and policies. This allows for an urgent and most often, short-term solution to handling calls without the cost and delay of new hardware or software acquisition.

We have provided a sample disaster recovery plan in the Examples of Previous Deliverables tab and, based on RESPONSE 150 from the Feb. 28, 2013, Q&A, will work with the Department to finalize the plan for the COMMIT project.

In-House Recovery

HP's dedicated disaster recovery team maintains current processes and forms to reflect the best practices. HP will use these as the basis for the processes and procedures customized for the COMMIT project.

HP maintains the following:

- Redundant, dedicated connections to our private Healthcare Network Cloud (HNC)
- Redundant connections to our U.S. Public Sector replication cloud
- Public Internet connectivity
- Diverse, account-dedicated (point to point) network connections.

This level of protection goes well beyond our competitors in the MMIS industry. The "In-house disaster recovery capabilities" stands above other competitive offerings. HP invests significant resources on disaster recovery and does not rely on a third party.

Secure Network

HP's dedicated, private Healthcare network and replication cloud, promote the highest level of security. These networks meet or exceed the requirements of the Colorado System Security Plan Template, as well as HIPAA Privacy and Security Guidelines. Secure VPN connections through the public Internet may be used, to provide the highest level of security available.

We will meet or exceed the disaster recovery and business continuity requirements in section 7.9 of the RFP, as evident by our experience in other states. After contract award, we will finalize and deliver a detailed plan that addresses the system, network, and office configuration. This final plan will allow the COMMIT project to run with zero to minimum disruption, in the event of a disaster; meeting or exceeding the expectations of the Department. HP also performs disaster recovery and business continuity testing, annually, at a minimum.

Reliability and Availability—Business Continuity During Regular Operation

HP invests substantial resources in hardware, software, networking, work force and expertise. Further, we cultivate a culture that promotes the availability of systems and services. This environment limits the need for diversion to an alternate operation-site when disasters occur.

Primary Data Center – Orlando



The primary data center for the Colorado interChange will be our Orlando Data Center facility in Orlando, Florida. It has an Uptime Institute Equivalent Rating of Tier III. We selected this facility to meet the demanding power and cooling needs of the next-generation computing environment with redundant power and cooling. This provides concurrent maintainability without the risk

of facility downtime. The Orlando facility hosts enterprise class devices for many HP healthcare customers with multiple layers of redundancy. Features include the following:

- Purpose-built data center fortress
- 130,000-square-foot facility
- Dual high-voltage utility substations
- Standard A- and B-side power
- N+1 jet turbine generators
- 85,000 square feet of 36-inch raised floor
- Staffed security 24 x 7
- Extensive video surveillance systems
- Diverse underground network access
- Support for water-cooled equipment

Additionally, our Orlando data center exceeds Tier III requirements with these additional Tier IV features:

- 24 x 7 staffing
- 50-80 build-out gross watt per foot
- More than 150 ultimate gross watt per foot
- Support systems separation within firewalls
- 100 percent support-space-to-raised-floor ratio
- More than 150 floor-loading pounds per foot
- No single points of failure
- 0.8 hours annual site-caused IT downtime
- Two active utility feeders
- Representative site availability of more than 99.995 percent

Our data center technical road maps automate routine, operational, and end-to-end processes and protect the business through resilient operations (business continuity and availability). The facility optimizes the use of energy, floor space, and cooling infrastructures (energy and space efficiency). The result is a next-generation data center with 24 x 7 adaptive infrastructure environments which provides better quality of service and business continuity.

Reliability and Availability During Disaster Recovery

We will use active locations in use for disaster recovery, in accordance with the requirements of the Department. HP uses a disaster recovery facility located in Colorado Springs.

Secondary Data Center (Disaster Recovery Facility) – Colorado Springs

This dedicated disaster recovery infrastructure is a raised floor HP data center contained in a full functioning data center campus facility. The facility is geographically remote from the Orlando production environment and contains office space and telephone infrastructure. HP staffs a dedicated disaster recovery team to support the Medicaid healthcare accounts.

Features of the Disaster Recovery Colorado Springs facility include:

- Located within a 21,000-square-foot HP data center
- Co-resident with the primary North American HP hardware, software, and networking response center
- Two utility power feeds from separate grids, and redundant backup diesel generators with fuel to support a minimum of 48 hours run time at full capacity

- 850-kilowatt uninterruptible power system (UPS) and redundant power feeds for the equipment
- Dedicated connections to the HNC, USPS Replication cloud and multiple vendor network capabilities available to provide redundant and diverse routing to major carriers (in support of specific customer requirements)
- Dedicated Enterprise and midrange SAN Storage with encryption at rest and “Near-real-time” data replication from the Orlando Data Center
- Dedicated and subscription resources (servers) available
- Public/Private web facing sites with SSL Certificates
- Keycard access
- Redundant cooling with generator backup
- Temperature and humidity control and central monitoring
- Dedicated full-time security personnel
- Video monitoring
- Full on-site disaster recovery rehearsal areas
- Centrally monitored independent fire control with five zones of smoke detectors and gas fire suppression under a raised floor

These data center facilities work together to maximize availability of the critical functions of the COMMIT project.

Call Center and Help Desk Operations

Effective communication between the healthcare community and the Department is essential to the success of call center and help desk activities. Our experienced HP team knows the business processes for recovery. Established plans and processes document our recovery, required resources, critical applications, and if components of the call center become inoperable.

We will base regular HP Call Center and Help Desk Operations for the Colorado interChange in Denver, Colorado using local customer services agents. While the agents will be physically located in Denver offices, the actual routing of the calls will be performed by one or more physical sites of HP’s designated HP Healthcare Call Center Platform. The HP Call Center Platform works throughout the United States to support the uptime requirements for the contract. We can enhance the platform, with expansion capabilities, which provides additional hardware, software, inbound trunks and capacity.

HP’s telecommunications infrastructure for the primary and backup connectivity is fully redundant, with automatic failover to support the reliability of this critical network.

We base our primary voice traffic on Voice over Internet Protocol (VoIP) or standard PRI telecommunications circuits. By building on this robust and proven technology, our network creates the optimal platform to support emerging IP services in the future.

The voice infrastructure system handles daily call processing, collection of call center statistics and averages, and self-service options to callers.

The following figure depicts a view of the HP Healthcare Call Center Platform with redundant connectivity.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

Redundancy of the Platform

The proposed HP Healthcare Call Center platform is built with a state-of-the-art shared telecommunications servers and gateways that can provide enhanced capabilities for failover and disaster recovery. We can configure the platform to provide dual processors, redundant network connections, power connections and local servers for survivability, based on the SLA (Service Level Agreement) requirements. Using this sophisticated platform will provide a level of availability for full business continuity to the call center and help desk. HP uses business continuity planning methodology to construct a plan for how critical functions will resume and within what time frame after a disaster or disruption. The disaster recovery plan covers the data,

hardware, and software critical for a business to restart operations if a natural or human-caused disaster occurs.

Besides the redundancy, we use IP-telephony and gateways which are technically part of the data network (LAN). This allows HP to use one or more of the following options quickly in case a disaster renders the dedicated operations building in Denver, CO inhabitable:

- Use IP-Agent Software and move the call center and help desk agents temporarily to an alternate location like a hotel that is safe for our employees
- Temporarily use call center and help desk agents who permanently work for other Medicaid accounts in other states

Print and Mail Services

In case of a disaster, HP will transfer our mail processing to an alternate existing HP healthcare site. If our primary office becomes unusable, we will immediately set up connection to another healthcare site, which eliminates the need for redundant large printer equipment on-site in Denver. One secondary facility option is the HP Oklahoma Medicaid account facility which performs the printing functions for many of our MMIS projects. It has the capacity for a night shift to resume the printing needs for the Colorado interChange MMIS.

Data Entry

If the primary data entry site is decommissioned, HP will activate alternative data entry within 24 hours of a declared disaster. Arrangements will be made to secure temporary space at an alternate HP facility or other temporary space to serve as our base of operations. We would install data entry terminals for our Denver data entry staffs' use at the location. This arrangement would employ a day-and-night-shift approach to handle the volume.

With the HP data entry staff members online, we can operate efficiently in our alternate site until the primary facility is operational. If the disaster continues, HP will obtain assistance from our other Medicaid accounts. HP is proud of our proven responsive disaster recovery services and its capabilities to help continue critical Medicaid services during emergencies.

Claims Processing

Manual Claims Processing

As live examiners process certain claims, this function will continue if disaster strikes. In the case where the primary operations site in Denver, CO becomes inhabitable, HP will continue operations with minimum disruption by installing computers in an alternative safe location; such as a nearby hotel. This arrangement would employ a day-and-night-shift approach to handle the volume.

In case the disaster continues for a long duration, HP will obtain assistance from other Medicaid accounts.

Claims Audit

Our claims auditors and the relevant quality control staff members will work from a remote location during a disaster event. These services will continue in the event of a disaster.

Development, Testing and Implementation of Changes

In our healthcare account structure, we do not have a single point of failure for the design, development, testing and configuration changes. In fact, we locate some developers and testers off-site so local issues will not affect them. Developers and testers can perform the tasks required so long as the servers are operational.

Documentation and Reporting

HP's policy is to maintain multiple back up documentation and reporting copies. The documentation of lessons learned for each enhancement and the incorporation of that information into the Change Management Plan will continue during a disaster.

Meetings

We have the technology, experience, and culture to regularly conduct meetings from remote locations, using HP Virtual Rooms or similar tools. This is a common practice in our healthcare accounts and will continue if a disaster occurs.

Business Continuity Plan and Disaster Recovery Plan (Unique ID 1023)

Please see the Attachment E - Examples of Previous Deliverables for a sample plan for business continuity and disaster recovery for the COMMIT project. The details of this plan will be finalized following contract award, approved by the Department and revised when necessary. This Plan also is discussed in detail in RESPONSE 31a.

- The plan will include the following information:
- Timely failover and redundancy
- Data recovery
- Claims/encounters processing
- Short- and long-term continuity operations
- Remote access (in accordance with Department standards)
- An alternate business site if the primary business site becomes unsafe or inoperable
- Source cause analysis reporting to the Department for unscheduled downtime
- Provide data backup
- Schedule and process for testing of the Business Continuity and Disaster Recovery Plan

HP will adhere to the Department's performance standards below, within the Business Continuity and Disaster Recovery Plan:

- Mission critical services (priority 1) will not be interrupted.
- Core services that shall be maintained with limited service disruption (priority 2) shall be recovered within eight hours.

- Systems and data where service disruption will cause serious injury to government operations, staff or citizens (priority 3) shall be recovered within 48 hours.
- 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) shall be recovered within five business days.
- Systems and data required for less critical support systems (priority 5) recovery time frame shall be mutually on by the Department and Contractor(s).
- The alternative site shall be fully operational within five business days of the primary business becoming unsafe or inoperable. The call center shall be fully operational within 24 hours.

Business Continuity and Disaster Recovery Plan Testing (Unique ID 1234)

HP will review and understand the Department's existing disaster recovery and business continuity plans. We will overlay our plan for the system and operations with flexibility, geographic diversity, and proven infrastructure. We will work together with the Department to provide the steadiness and continuity of operations while taking the appropriate steps toward system backup.

During the development of the COMMIT projects Disaster Recovery infrastructure, the HP Disaster Recovery Team will work with the Department to develop the technical recovery plan (TRP) for the production environment. In our regular practices for the healthcare accounts, the plan is used throughout the Disaster Recovery planning process; from the development of the disaster recovery plan to disaster recovery rehearsals, including actual recovery events. The TRP includes document versioning, contact information for the Department and HP personnel, technical team assignments, platform component details, facility location information, a recovery checklist, and pre and post rehearsal activities list.

We will perform the disaster recovery and business continuity test annually for the Colorado interChange MMIS. It is our standard practice to review the disaster recovery plan against the TRP during each periodic rehearsal. The rehearsal team, consisting of participating clients from the Department and HP, perform this review. During this review, the infrastructure configuration information, such as hardware, software, and network information, is verified and updated to promote alignment between the documentation and the current production infrastructure. Previous rehearsal and procedures notes are reviewed and updated to verify the latest standard and best practices are incorporated.



HP will develop and follow robust Business Continuity and Disaster Recovery plans customized for Arkansas' needs. When natural disasters threaten the local landscape and hardware, account teams can tap the HP Corporate Crisis Management team for additional support.

348 124 03_0513

The range of infrastructure and services responsibility covers events from partial loss of function or data for a brief amount of time, to a “worst-case” scenario in which a disaster even results in a data center failure.

HP uses a corporate wide operations alerting system, the “Response to Operational Problems” (RtOP) to support incident management; including but not exclusively supporting disaster recovery. The system is based on varying degrees of severity which is determined by the business impact and is aligned to the Department’s requirements and definitions. If a disaster event or other high-impact unscheduled downtime occurs, the appropriate HP capability, such as the storage, backup, network team or other, will perform a source analysis.

A periodic disaster recovery exercise will be performed. A specialist project manager is allocated to the account to run the drill. The activities include the following:

- Working with the Department to define the exercise specific objectives
- Reviewing and updating the current state production against the recovery documentation
- Performing a simulated end-to-end recovery in isolated infrastructure, using current point-in-time production data
- Providing documented evaluation and rating of the exercise
- Creating postmortem review of the exercise and opportunities for improvement – in both the process and the execution of the rehearsal. This single effort provides both the Department and HP with the ability to constantly improve and share the best practices among HP’s healthcare accounts.

The Department may request that specific tests be performed and supporting documentation (for example, screen prints for a query) presented of the outcome. The Department may prefer to participate in the rehearsal testing. The results of the tests are recorded and reviewed in subsequent rehearsal exercises.

As part of the Disaster Recovery rehearsal process, a document review is performed before the rehearsal. Items reviewed during this process include the technical recovery procedures, the build of the production environment, and technical documentation. The BC and DR plans will be updated to reflect any changes made. These updates are then validated during the rehearsal with issues or gaps being identified and resolved. Additionally, after each rehearsal, the team performs an evaluation, identifying what worked well, where issues were encountered and suggestions for future rehearsals. HP will provide results of the Business Continuity and Disaster Recovery tests to the Department.

The Department staff members or designee will be allowed to participate in testing, if requested by the staff. HP will comply with this requirement, in accordance with its own security rules and regulations surrounding the need for physical access to HP’s data centers by the Department staff members or their designee.

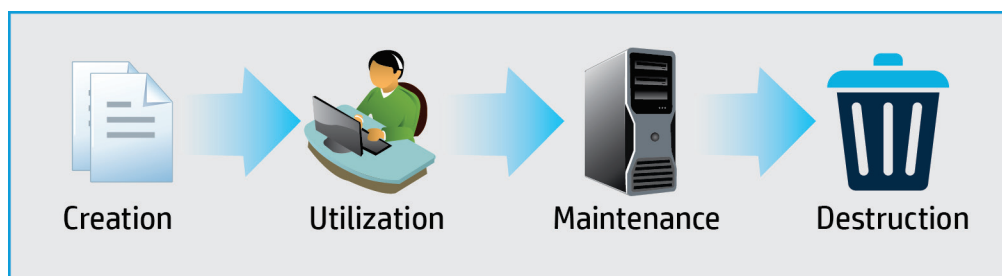
RESPONSE 38i

7.10 – Data Retention Requirements	In Production? YES/NO
Description Addresses Requirements (Provide the range as applicable): 1236-1247	YES

Data retention encompasses the efficient and logical governance of the receipt, maintenance, use, and disposition of records—paper or electronic. Capturing and maintaining evidence of, and information about, business activities and transactions is critical to Colorado Medicaid. Effective data and records retention management helps the Department promote compliance with federal and State laws and regulations, and prevent the unintentional destruction of records. HP understands the importance for the Department to retain documents for CMS inquiries, legislative inquiries, managed care history of payment, or court cases.

A records life cycle comprises many phases, from creation to final disposition and destruction. HP has been responsible for data retention for more than 40 years and is responsible for Medicaid data retention in 20 states. We understand your business drivers and can be trusted to be the custodian of your data. As the following figure details, we protect and secure data during the entire document life cycle.

Document Life Cycle



348_125_02_0413

The American Health Information Management Association (AHIMA) Body of Knowledge states the best data retention policy comprises the following:

- Verifying information is available to meet the needs of continued patient care, legal requirements, research, education, and other legitimate uses of the organization
- Guidelines that specify what information is kept, the time period for which it is retained, and the storage medium on which it will be maintained—such as paper, microfilm, optical disk, or magnetic tape
- Clear destruction policies and procedures that include appropriate methods of destruction for each medium on which information is maintained

HP follows these same guidelines in creating our base processes and procedures in our best practices repository. We will apply State specific rules and regulations to create the Colorado Data Retention section of the operations procedures plan.



Our HP data centers have full-time backup and recovery administrators who are responsible for the hardware, software, and services related to storage, backup, and recovery of file data. The HP hosting facility's backup services are operational and is included as part of the hosting service contract. HP provides the full gamut of backup services; from full servers to a full file system level. The database servers include full backups of the database tables, logs, and other recoverable tables needed to restore an entire database or a single table.

The backup service includes backups to tape media or disk. Tape media supplies a backup of a point in time and is stored off-site in various rotations at a secure facility. Disk backup is faster and is usually integrated with tape. For instance, if there is a large database, a disk-to-disk copy can be completed in minutes, thus the time lost for updates to the database is small, while the copied database is moved to tape for more permanent and off-site retention.

The backup cycles we typically employ on Medicaid accounts include daily, weekly, and monthly. The daily backups are incremental and only completed for files that changed. The weekly and monthly cycles are full backups in which the files are completely copied to tape; regardless of whether they changed. The files on tape are rotated to an off-site location so that the most current copy is off-site while a previous copy is returned. HP will adapt our cycle schedules to fulfill the Department's specific backup requirements as defined during the Discovery and Requirements Validation/Requirements Elicitation Phase.

HP will follow our well-established Healthcare Enterprise EDGE SDLC processes during the phases of the COMMIT project, including data retention requirements. HP will perform the following high-level tasks during the Discovery and Requirements Validation and Requirements Elicitation Phase to deliver a data and records retention system:

- Review Department regulations and rules regarding data retention
- Work with the Department to fully document relevant federal and State regulations and rules, and further define the requirements in Appendix A – Requirements and Performance Standards Matrix, Section 7.10
- Enter the following requirements into our shared project plan template:
 - Document data retention processes and procedures operations procedures plan
 - Implement, test, and deploy data retention policies within the MMIS
 - Apply retention policies to converted data and transferred records
 - Implement policies to manage the retention of paper records
 - Define schedules for archiving and purging records

- Document the project management and system artifacts and store in the appropriate repository—HP PPM, HP ALM, or SharePoint

When established, HP will apply policies to the data, records, and documents of the Colorado Core MMIS and Supporting Services project during the Operations and Turnover phases.

Data for Reporting and Analysis (Unique ID 1236)

In accordance with the operations procedures plan, HP will maintain provider, client, claims or encounters processing, benefit utilization, financial, reference, and other data to support management reports and analysis. This is core to what interChange does; it is the backbone of what our Medicaid accounts use to run our businesses and what the Department will use.



The Colorado interChange Medicaid Enterprise system solution is designed to maximize the availability of data in a real-time environment where users have online access to the data needed to perform their MMIS operational tasks. Through our data architecture, including the data partitioning, we can maintain system performance levels while retaining vast stores of data.

Provider and Client Data (Unique ID 1237)

HP supports MMISs in 20 states today. Through our Medicaid experience we understand the importance of content retention for the State-specified length of time, make it readily accessible, and securely destroy unneeded material.

During the transition planning meetings, a list of historical records in the custody of the incumbent fiscal agent will be developed, reviewed, and modified as needed. This list will serve as the basis for the final historical record transition checklist, when the records are physically transferred to HP.

We will maintain current and historical provider and client records according to Department specifications—paper and electronic. Whenever possible and permissible, we will convert paper documentation into a digital format. We will document the processes in the operations procedures plan.

Records in Litigation (Unique ID 1238)

HP fully understands the criticality of documentation related to matters of litigation. The Department must satisfy legal obligations to retain records and satisfy regulatory requirements to keep certain types of data, sometimes indefinitely.

We have supported numerous customers in retrieving documents for legal discovery motions and evidence in legal proceedings. HP understands the need to maintain those records after litigation, as instructed by the court or desired by the Department. We will comply with the schedules and time frames the Department outlines. HP will document the processes for record retention of litigation materials in the operations procedures plan.

NDC and HCPCS/CPT Crosswalk (Unique ID 1239)



HP delivers a National Drug Code (NDC) to HCPCS/CPT crosswalk in the Colorado interChange solution. The NDC procedure code cross-reference is maintained on a table with effective and end dates. Updated data is date-segmented so historical records can be maintained. Data is updated quarterly and updates are made through an MMIS panel or as a file upload for larger updates. Crosswalk data can be used for claims and drug rebate processing. Additionally, we will maintain current and historical crosswalk files for the agreed-on retention period.

We will document the processes and procedures for maintaining the crosswalk in the operations procedures plan.

Retain Paper (Unique ID 1240)

HP innovation in the area of document imaging is unmatched by our competitors. We have shared technology from the banking industry and adapted it specifically for Medicaid-related document processing. Our fiscal agent states using the interChange solution we are bringing to the Department are seeing productivity improvements and image quality enhancements.



As paper is scanned and images captured, the original documents are placed in numerically sequenced batches and filed by Julian date for later retrieval if necessary. Following Department approval, HP leadership will routinely authorize the secure destruction of original documents that have a human-readable electronic copy in the image repository.

We will work with the Department during the Discovery and Requirements Validation and Requirements Elicitation Phase to align the paper record management requirements and the preferred archive process to efficiently and properly adhere to the Department-specific periods and retention guidelines.

Purging, Archiving and Protecting (Unique ID 1241)



HP knows the importance of letting an organization control the aging of its records so it can conduct an orderly disposal of unwanted records or archive its important records for future reference. HP will use Department-specific disposal and retention schedules to manage file retention and archiving.

Disposal can mean alteration, transfer of custody or ownership, or destruction of agency records. For government records, a disposal authority is a legal instrument that gives agencies and organizations approval to dispose of records. A schedule is an instrument that allows the legal destruction, long- or short-term retention, transfer, or alteration of an agency's records. Triggers defined by the schedule enable HP to calculate transfer and destruction dates. A single retention schedule can contain multiple date triggers—for example, transfer to an interim archive five years after closure and then destroy 10 years after closure.

Our approach to periodic content archiving, maintenance, and storage is a coordinated method that uses interChange for primary storage of data records and our EDMS solution for storage of images and reports. Our solution contains archiving features that will be managed through routine processes that we will work with the Department to define. Recognizing the need to archive older electronic content, we offer a storage management system and a means to contain storage growth.

Besides the business values of archiving through periodic removal of information from the MMIS, we experience operational efficiencies, such as reducing the time required for backup and recovery activities. Active archiving enhances the performance of production databases by eliminating records that are not accessed daily but may be needed for reference occasionally. The operations procedure plan will clearly outline the requirements for purging, archiving, and protecting data from destruction. When outlined, HP will rigorously adhere to the requirements.

Media for Retention and Archival (Unique ID 1242)

HP will retain and archive required data and documents in the electronic media format as specified by the Department. The operations procedures plan will document the preferred storage medium on which each document type will be maintained—for example, optical disk or magnetic tape.

HIPAA Compliance for PHI (Unique ID 1243)

Stored PHI will be encrypted or protected according to industry standards, including data at rest in the MMIS and backups. The Colorado interChange provides encryption behind the scenes with minimal impact to system performance.

Although the HIPAA privacy rule does not include medical record retention requirements, it does require that covered entities apply appropriate safeguards to protect the data. HP will adhere to State laws that govern medical records retention.

HP follows industry best practices regarding scheduled backups and managing incremental and full backups for optimal performance and security. The NetBackup Master Server controls the loading and unloading of tapes and other access to the tape library. Tape pools are set up on a per-customer basis and enforced by the NetBackup Master Server.

The Master Server also is responsible for creating, managing, and distributing customer encryption keys used to encrypt and decrypt tape media and media metadata. The media servers request these customer encryption keys from the Master Server using the metadata communication channel as part of their backup and restore jobs.

The Master Server keeps a master catalog of metadata, which is stored in a storage array attached to the backup SAN. The arrays holding the master catalog are copied through an automated SFTP process to the disaster recovery site, validating the master catalog's availability in the event of a disaster.

Access to the media servers and Master Server is strictly controlled on an “as-needed-only” basis and monitored from the monitoring tools deployed at the HP data center. Standard monitoring tools used to monitor access to the backup environment include syslog, ArcSight, and Network Intrusion Detection software or devices.

The operations procedures plan will include policies and procedures for prevention of improper alteration and destruction of PHI and guidelines for access, retrieval, and duplication of sensitive data.

Retrieval and Access for Documents and Files (Unique ID 1244)

HP is committed to having the right information in the right place at the right time to make sure the operation of the Colorado Medicaid program is smooth. Users must be able to retrieve documents quickly and accurately. The HP document solution combines interChange and IBM OnDemand Document Management to modernize the business processes and professional services. The result fulfills the Department’s standards and federal and State compliance guidelines for secure storage and retrieval of documents. The overall solution provides scalability for future requirements and changes.



The Master Server keeps a master catalog of metadata, which is stored in a storage array attached to the backup SAN. The array holding the Master Catalog is copied, through an automated SFTP process, to the disaster recovery site, verifying the Master Catalog’s availability if a disaster occurs.

HP will work with the Department to identify document retention specifications. We will allocate sufficient space to store documents online for the required retrieval parameter of six years, eliminating the need for a separate archival and retrieval process. Archived documents more than six years of age will be maintained for the life of the contract and returned to the Department or successor vendor during the Turnover Phase.

Indexed Archive (Unique ID 1245)

Our solution to archiving considers the Department’s need to access critical MMIS data readily and maintain system performance standards. Our solution does not archive MMIS transactional data; we retain the data in the online database rather than archiving it. MMIS data will be available when users need it.

Archives of non-MMIS data, such as documents, are handled through Microsoft SharePoint and indexed in a directory view. As required in the RFP, requests for archived data will be

45 CFR 164.530(c)

(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2)(i) Implementation specification: Safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

acknowledged within 5 business days and fulfilled within 30 business days of the request.

Archive Management (Unique ID 1246)

HP supports indefinite retention of data and records using our storage and archival methodology while preserving system performance. We recognize that there are business reasons to purge data and will enable the Department to manage this event in an orderly fashion. Though our systems can schedule purges, HP will never purge data, records, or documentation without a strict review process and approval from authorized Department personnel. During the Discovery and Requirements Validation and Requirements Elicitation Phase, HP will review the purge options and document the best strategies for each type of information in the detailed retention and purging schedules.

Conversion Claims (Unique ID 1247)

The standard HP conversion process enables users to search for and retrieve converted claims using the original legacy transaction control number (TCN). The conversion process creates a legacy TCN to internal control number (ICN) cross-reference table that links the original TCN to the converted claim ICN.

RESPONSE 38j

7.11 – Technical Requirements	In Production? YES/NO
Description Addresses Requirements (Provide the range as applicable):	N/A

As healthcare enters the era of the Affordable Care Act (ACA) and Medicaid Information Technology Architecture (MITA), the role of the Colorado Medical Assistance program will become increasingly important to supporting future growth and information exchanges.

The following table provides a high-level summary of how the HP solution meets the Department's requirements of 7.11.1.

HP's Solution Benefits for the Department

State Requirement	Solution	Road Map
Modern system to support the business functions of the Colorado Medical Assistance program and other supporting programs	The HP interChange MMIS is a MITA 3.0 technical infrastructure that has been certified by CMS under the new MITA standards. We operate interChange in 13 states.	EMS Goals and Objectives Colorado Medicaid Program and MITA Impact of ACA on Colorado Medicaid Program Business and Technology
Solution based on business processes, business rules, and data and metadata management that promote a modular component based design.	The HP solution is built on business processes using the k2 blackpearl workflow, HP @neTouch, rules engine, and Benefit Policy Administration (BPA) rules engine. HP maintains and uses physical, logical, and metadata models of the tables, interfaces, screens, and user interfaces. The HP Colorado interChange solution is a component-based design using HP MMIS-specific services and various commercial off-the-shelf-based (COTS-based) products such as document management (IBM OnDemand), workflow (blackpearl), rules engine (Corticon), correspondence management (HP Exstream), electronic data interchange (EDI) (Edifecs), service-oriented architecture (SOA) (Microsoft BizTalk), contract management	Modular Components Moving Toward a MITA-Oriented Medicaid Approach

State Requirement	Solution	Road Map
	(HP PPM and HP ALM), and others connected through a SOA.	
Interoperable across components and with external applications and data	<p>The MMIS solution is a SOA that connects services with an enterprise service bus (ESB). The ESB has connections to B2B business data transfer and the healthcare HIPAA sets of data, where we use Edifecs.</p> <p>The HP File Tracking System (FTS) tracks the interface and messaging through the ESB.</p>	Modular Components

Department Goals and Objectives

HP will work with the Department to implement a flexible, scalable Core MMIS with the proven ability to streamline business processes. HP's solution supports the Department goals and objectives for the COMMIT project, as shown in the following table.

Department Goals and Objectives

Goal	HP Colorado interChange MMIS Solution
Use Medicaid MMIS funding to integrate the Department's processes and systems using business processes and workflow	<p>interChange provides functions to support multiple agencies and integrates COTS tools that can be shared across the MMIS operations and systems.</p> <p>As a multipayer system, interChange enables multiple agencies to cost-effectively process the healthcare transactions through a single system.</p> <p>interChange Connections provides interoperability by providing data transformation and rule-based management at the field or file level.</p> <p>The MMIS solution provides total Single Sign-On (SSO) to each system and subsystem, allowing users and other departments to connect into applications or activities that they have been approved for.</p> <p>We incorporate workflow into the business processes to automate functions that are rules-based and provide workflow so that staff members can manage and track their work queues and loads.</p>
Increase the maturity of business processes and supporting systems pursuant to the MITA	interChange provides integrated workflow tools to streamline and standardize operational business processes. MITA Business Process Steps are available online through the MMIS user interface @neTouch Help system.

Goal	HP Colorado interChange MMIS Solution
Maximize efficiency in operational costs with simplified processes and systems	<p>interChange reduces costs through automated workflows and user configurability. Advanced workflow reporting provides operational insight to transform process efficiency.</p> <p>By using the Rules Engine to define processes through screen updates, business staff members can make policy changes and test them without requiring a programmer.</p>
Create client and provider interactions that are clear and concise	<p>Client and provider self-service options are available to improve overall program satisfaction and deliver the CMS vision of a 21st-century healthcare experience for the stakeholders.</p> <p>The Client Portal allows access by clients to services through an intuitive user interface, context-sensitive help, and Frequently Asked Questions.</p> <p>The Client and Provider Portal is ADA/WCAG-compliant for people with disabilities or other handicaps.</p> <p>Additionally, the integration of the HP Exstream tool allows the automatic generation of correspondence with clients and providers using templates that have been customized for clear, concise communication.</p>
Data integrity and data management	<p>interChange uses data models for logical and physical data and metadata descriptions of the table entries. The meta data models include the HIPAA healthcare transaction sets, other X12, and other Extended Markup Language (XML) metadata descriptions.</p> <p>interChange uses data cleansing and other ETL processes to build back and convert the historical data to the HP MMIS.</p>
Provide robust, secured data exchange and connections to external applications	<p>interChange provides a proven data model and business exchange framework to support smooth, secure data exchanges. Data validation services support data cleansing and semantic consistency.</p> <p>Connectivity and Security using an ESB allow coupling to external systems or data.</p>
Advance the State forward toward higher Seven Standards and Conditions (7SC) and MITA Maturity.	<p>HP provides an MMIS that has been certified with a workflow, rules engine, SSO, EDI, and document management services in an SOA framework. With this MITA-compliant framework, the Department and HP can engineer the business processes to be more automated and streamlined to increase the level of MITA maturity and elevate the compliance with the 7SC.</p>

Modular Component Design

In the following sections, we present the proposed Colorado interChange and its modular component design. The proposed solution provides interoperability and easy connectivity to outside entities and infrastructure. The component architecture lends itself to incorporating technology through exposed business interfaces and easily connecting to external applications or data sources.

Colorado interChange Application Architecture

Through the Colorado interChange architecture solution, the Department can respond faster to regulatory, programmatic, and technology changes because HP's proposed technical solutions and services are standards-based, adaptable, and extensible. A combination of proven approaches to security and privacy and the technical and business architecture provides easier access to data and information across the MMIS. At the heart of the Colorado interChange is the CMS-certified Wisconsin MMIS, the first MMIS to successfully be evaluated and certified through the new CMS certification process. Throughout the application architecture, COTS packages are integrated with the MMIS to present service-based modules. The result is an efficient, business-feature-rich solution for the users.

The Colorado interChange also contains our secure, public-facing web portals as the access channel for clients, providers, and trading partners. CMS reviewers identified the business services provided through the HP web portal as a best practice during the MMIS certification for the Florida interChange system. The blue boxes in the following figure are interChange modules that align to the MITA 3.0 operational areas. The interChange Business Services framework (vertical and horizontal gray bar in the figure) are the business operation services and include workflow, web services, business rules, and the inSight Dashboard reporting. This component uses XML to transport and store business language data and instructions to the individual services. This component provides the synchronization and orchestration across and among the various services.

The gray vertical bars are the COTS products whose services are exposed to use by the business processes or web services and include document management, correspondence management, workflow, business rules engine, and interChange Connections.

The interChange Connections contains the enterprise service bus (ESB), HIPAA translators, HP FTS, and the B2B connectors. interChange Connections provides the internal wiring and bridge infrastructure to connect and manage the technical services. These services are integrated by the



In Wisconsin, the interChange MMIS has demonstrated its adaptability and capability to support changes in the healthcare program through the implementation of 1,000 work items in less than a year. Forty-one of the work items have accounted for an estimated savings of \$350 million in benefit expenditures.

348 133 02 0313

interChange Business framework. The interChange Connections separates the technology layer from the Business layer.

Contract management is the grayed rectangle and integrates the HP PPM, HP ALM, and SharePoint together to provide a continuous view of the requirements, status, and test results. Test results and project plan information is consolidated into single view application.

Finally, the purple colored bars represent the various external stakeholders.

Colorado Medicaid Program and MITA

The traditional MMIS offers vast functions and a single point of contact and integration, but states recognize that niche vendors often provide specific capabilities—such as pharmacy benefit management and business intelligence—that enhance traditional functions. The MMIS must provide the connective tissue between traditional and niche components. Colorado is procuring and combining pharmacy benefit management, business intelligence, case management, and core MMIS functions into the comprehensive Core MMIS and Support Services solution.



The primary function of the MMIS is to support state healthcare business, including claims processing and tracking clients in managed care. At the same time, it sets the foundation for advances in MITA maturity to help the Department meet changing industry standards. HP and our industry-leading technologies (as evaluated by Gartner and Forrester) offer Colorado the

following advantages:

- An advanced SOA-enabled Medicaid system, recently enhanced to support states' efforts to meet the CMS 7SC, including MITA 3.0
- Flexibility needed to keep pace with evolving budgetary, regulatory, and CMS requirements
- Functional capabilities that let Colorado take full advantage of current Health Information Technology (HIT) and the Colorado Regional Health Information Organization (CORHIO) Health Information Exchange (HIE) to better serve clients, stakeholders, and providers
- A CMS-certified MMIS, experienced staff members, and our implementation best-practice repository that are proven to deliver consistent results and on-time implementations

Moving Toward a MITA-Oriented Medicaid Approach

The HP teams have embraced MITA principles when enhancing the interChange system—proactively aligning our operational and technical architectures with the most recent MITA principles as they emerge. Now we are bringing CMS 7SC into focus, enhancing interChange to help states communicate with CMS about 7SC to obtain federal funding.



The foundation provided by HP's proposed Colorado interChange will enable the Department to mature with the evolving MITA 3.0 principles during the federally required five-year plan. The following table shows some of the enhancements for the interChange system regarding 7SC.

Proposed interChange Features and Corresponding CMS 7SC

Colorado interChange MMIS	CMS 7SC
User Interface (UI) enhancements —@neTouch functions significantly enhance staff members' productivity. Now the information is available at the touch of a button.	<ul style="list-style-type: none"> • Business Results Condition—System efficiency
EDI/ESB Application Integration —The interChange Connections solution simplifies sharing standard transaction sets with trading partners through the ESB, FTS, HIPAA compliance validation, and monitoring framework.	<ul style="list-style-type: none"> • Interoperability Condition—Data sharing • Modularity Standard—SOA, loose integration
Workflow Management —interChange workflow standardizes business processes and enhances efficiency, optimizes outcomes, and brings greater maturity to the MMIS concept of operations.	<ul style="list-style-type: none"> • MITA Condition—Concept of operations, workflow • Business Results Condition—Automation and standardization of business processing
Correspondence Management —HP Exstream uses open application program interfaces (APIs) and will be deployed as cloud-based software as a service to generate correspondence.	<ul style="list-style-type: none"> • Leverage Condition—Cloud, commercially available components • Modularity Standard—Open APIs
Performance Reporting —Colorado interChange MMIS inSight module for advanced dashboard style reporting for system, business process, and program metrics.	<ul style="list-style-type: none"> • Reporting Standard—Performance standard reporting
API, Modularity, SOA —Clearly defined APIs connect interChange components. McKesson VITAL, HP Healthcare Portal, HP Exstream, OnDemand, and interChange inSight dashboards expose and use these APIs to perform their features as part of a SOA.	<ul style="list-style-type: none"> • Modularity Standard—SOA, open APIs, modular components

interChange functions align to the business areas recognized by MITA. We built our processing platform on a true SOA, supported by web and business services. Through data translation adaptors, we can readily transform data from one format to another, allowing a more interoperable data exchange. A successful MMIS solution will enable the Department to keep its commitments to Coloradoans—delivering user-friendly service to providers and clients; focusing on providing preventive care; maintaining accountability of resource usage; and verifying that clients have access to appropriate, high quality, medically necessary healthcare.

Impact of ACA on Colorado Medicaid Program Business and Technology

The ACA significantly influences the Colorado Medical Assistance program by defining necessary programmatic changes, promoting streamlined business processes, and emphasizing technology and standardization to create smooth interactions across the healthcare continuum. Specifically, Colorado Medicaid business and technology will be affected by the following ACA requirements:

- Mandates changes in eligibility determination
- Mandates standardized essential health benefit packages
- Increases the number of individuals eligible for Medicaid
- Drives strategic change through CMS innovation
- Drives opportunities for payment reform, such as accountable care organizations
- Enhances program integrity efforts
- Drives industry standardization

It is difficult to know exactly what transformation will be required, but these changes will manifest in increased financial pressure and increasing demands for service. Because of ACA and similar healthcare legislation, Colorado requires a technical architecture that enables administrative and benefits savings through its flexibility and self-service capability. To balance these forces of increased demand and financial pressures, Colorado requires a technical architecture that promotes the following features:

- Streamlined business processes
- Improved self-service for stakeholders—especially providers and clients
- Enhanced benefit plan management
- Reduced cost to adopt industry standards and federal and state legislative mandates



HP's proposed Colorado interChange provides the State-required technical architecture to meet the challenges and opportunities of ACA. HP is proactively evolving MMIS business functions following MITA, ACA, and 7SC guidelines as we add advanced features and architectural capabilities.

The following features of the Colorado interChange will increase efficiencies, reduce manual efforts, and advance the maturity level of processes:

- Supporting multiple payers
- Integrating with LexisNexis for provider credentialing and background checks
- Permitting authorized business users to configure benefit plans
- Supporting integration with HIEs
- Supporting real-time eligibility updates to keep critical data current
- Supporting compliance with industry standards through Edifecs editing
- Expanding provider and client self-service, reducing the administrative costs

- Facilitating disease and care management through the McKesson VITAL component
- Providing a rules engine for categorizing eligibility and determining Modified Adjusted Gross Income entitlements

ACA defines an evolving set of legislation and standards that will be implemented during the next several years. The Department requires a flexible, extensible healthcare management platform to keep up with those changes. HP's proposed Colorado interChange provides a scalable architecture that can easily grow and change with the Department.

Configurable Solutions with Minimal Customization

The overall purpose of the technical architecture, as defined within MITA, is to provide a layered, modular healthcare solution for greater overall flexibility. With modular features such as the specialized client and provider portals and the module for prior authorization management, the Colorado interChange solution more than meets the Department's needs. The Colorado interChange architectural solution provides a logical separation across layers that are implemented independent of the underlying platform and includes services that support the various layers and component interaction. The services are initiated using standard methods in the invocation of the functions supported.

The overall architecture schematic in the following figure provides an overview of the Colorado interChange application architecture, its functional layers, and how the interoperable layers relate to each other.

The presentation layer depicts the various access channels that the stakeholders have to the solution. The stakeholders have access through @neTouch to configure their individual access favorites including screen navigation. The BPA enables the business staff members to define the rules for the benefit administration, eligibility, and claim payment without the need of programming or large volume testing. The portals contain numerous self-configured processes with intuitive screens to facilitate setups.

The application services layer comprises the interChange Business Services Framework. The Business Services Framework comprises interChange Connections and interChange Workflow. Connections provides secure and highly efficient management of healthcare data sets and the business to business connections required to manage the new-generation MMIS. interChange Workflow orchestrates human and machine-based business activities. The business analyst specifies the workflow parameters and defines the business rules for each stage of a business process.

The integration layer articulates the use of the base HP interChange solution and the proven COTS application components integrated within the overall solution. The overall interChange MMIS uses many COTS packages—to improve readability, the figure documents the most commonly referred-to packages. The Colorado interChange is the SOA-enabled solution that best positions the Department to continually mature the business processes the MMIS supports.

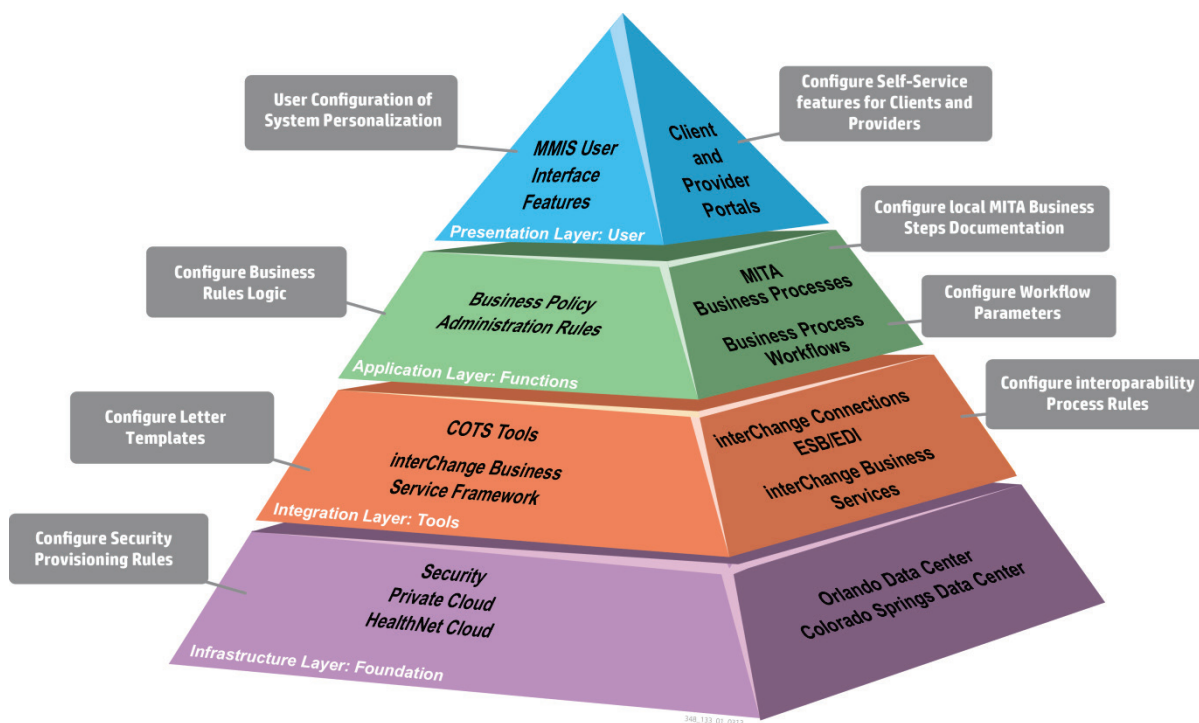
In this layer, the letter templates can be configured and the interoperable process rules are defined.

The infrastructure layer contains the facility, servers, network, and security services. These are where the heterogeneous technologies run. The integrated configuration keeps the business applications separate from the infrastructure. The security is set up for the servers, network, and data transport modes through configured processes.

Our MMIS is built to foster adaptability to evolve as state healthcare programs change—from our BPA configuration features to the integration of configurable COTS packages, such as a rules engine, for specific business value functions. The solution can be adjusted and configured to meet changing business demands as healthcare in Colorado changes across time.

The figure details the integration between the layers of the MMIS, including external stakeholders. This configuration results in a solution that is flexible, configurable, and scalable.

Integrated Configurable Solution Components



Using best-in-class COTS tools delivers value-add business features throughout the various MMIS business areas. The following figure provides a cross-reference of the shared services we reuse across the defined MITA business areas and the nine functional areas. The rules and workflow and ESB tie the nine functions to the MMIS business areas through service-based interactions. The following figure provides a clear picture of how services are integrated and reused throughout the overall Colorado interChange solution.

Colorado interChange COTS Integrated Solution per MITA Business Function

	Document Management	Communication	Content Management	Rules and Workflow	ESB
Client Management	●	●	●		●
Provider Management	●	●	●	●	●
Operations Management	●	●	●	●	●
a. Service Authorization	●	●	●	●	●
b. Claims/Encounter Processing	●	●	●		●
c. Financial Management	●	●	●	●	●
d. TPL		●	●	●	●
e. Reference Management			●	●	●
Contractor Management	●	●	●	●	●
a. Managed Care	●	●	●	●	●
Business Relationship Management		●	●		●

348_128_01_0013

Rules-Driven Design

The MMIS uses table-driven updates for eligibility, pricing, edits and audits. This is further coupled with a BPA rule processor that can be associated with providers, eligibility, and pay packages to pay a claim. The following figure illustrates the full level of control the authorized business user has to set up the policy, including the edits and audits needed to be satisfied. Users can easily enter this information into a screen.

The MMIS design supports a state-of-the-art rules engine that allows direct integration of business rules into the workflow using web services and the K2 blackpearl workflow. The rules engine allows entry in business language to GUI-based screen. Security is interconnected through the role-based access.

Configuration Approach

The HP Colorado interChange solution is set up so that configured services go across the MMIS and facilitate easy setup by the system's average business user. In the subsections that follow, we will highlight two specific aspects of the configuration for this response. In the first section we will detail @neTouch in the UI and how users can configure the Favorites so the MMIS is now personalized to the individual business user's specific business functions. The ensuing section details the BPA and how business users can easily configure the rules.

@neTouch

The interChange MMIS has delivered browser-based UI capabilities for years. Because we have such a broad number of interChange installations, our teams have the advantage of pulling in user experience information from many locations. Based on this user feedback, we have made user-defined enhancements to the interChange UI. These changes are called the @neTouch

family of features, and they enable users to personalize the MMIS to their specific roles and make navigation within the system easier than ever.

@neTouch Defined

HP built the @neTouch family of features based on guidance from our business experts who perform the detailed tasks every day. Healthcare is complicated, but navigating to what users need when they need it is now intuitive, fast, and context-sensitive. HP's business awareness and enhanced solution features simplify the user's tasks in interChange. @neTouch navigation provides quick and timely access to the following favorite items:

- Context-sensitive business screens
- Configurable favorite links
- Consolidated content profiles for viewing or printing
- Context-sensitive help
- User-controlled features through online configurability at the personal level

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

How @neTouch Will Benefit the Department

The @neTouch Access feature provides dynamic, context-sensitive, single-click navigation to the most relevant screens based on the current business process being worked.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**



In a call center, speed is critical. Navigating through complex menu trees takes time. Users need immediate access to supporting, related data from across the system to answer questions. For example, a call center agent is talking with a provider about a claim that has been denied. While on the claim screens, new navigation controls provide direct access to a vastly expanded set of data related to that specific claim as follows:

- **@neTouch**—The provider screen with other data, type, and specialty and contract tabs displays.
- **@neTouch**—Specific client information, their eligibility, and their primary care physician appears.
- **@neTouch**—Error code details, disposition, and resolution information appears.

How @neTouch Works

With user customization at their fingertips, @neTouch Favorites provides personalized access that makes staff members more effective.

RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED

Each individual accesses certain screens frequently, so the user can pin screens used most often to the Favorites list. Essentially, each user can configure an MMIS favorite navigation menu.

Users do not have to navigate through the menu tree to access their favorite screens or searches. The Favorites information link at the top of interChange MMIS expands the favorites drop-down at a click and retracts with a second click. Favorites include Favorite pages and Favorite searches as follows:

- @neTouch and the Favorites window opens.
- @neTouch and your desired screen opens.

Adding a Favorite page is the same in interChange as it is at home in a web browser. Users simply click the “Add Favorite Page” button when a screen they use often is open in the work area pane. Reduced clicking through navigation menus allows staff members to access frequently used pages faster and more easily, making them more productive and efficient. Improving efficiency at the task level of the interChange MMIS enhances overall staff effectiveness.

@neTouch offers Profile to View or Print. This feature produces a preconfigured profile or snapshot of data based on the selected entity such as a provider or a member. Profiles can be configured by users for each business area—for example, different information can be presented on the physician or hospital profile. As the following figure details, interChange generates profiles in PDF with a single click of the Print button to view, save, or print as needed.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

Our business users defined the @neTouch Profile to achieve a simpler way to record a snapshot of information. This feature replaces the need for cumbersome screen prints and delivers custom-configured PDF output in a separate browser window to support business functions.

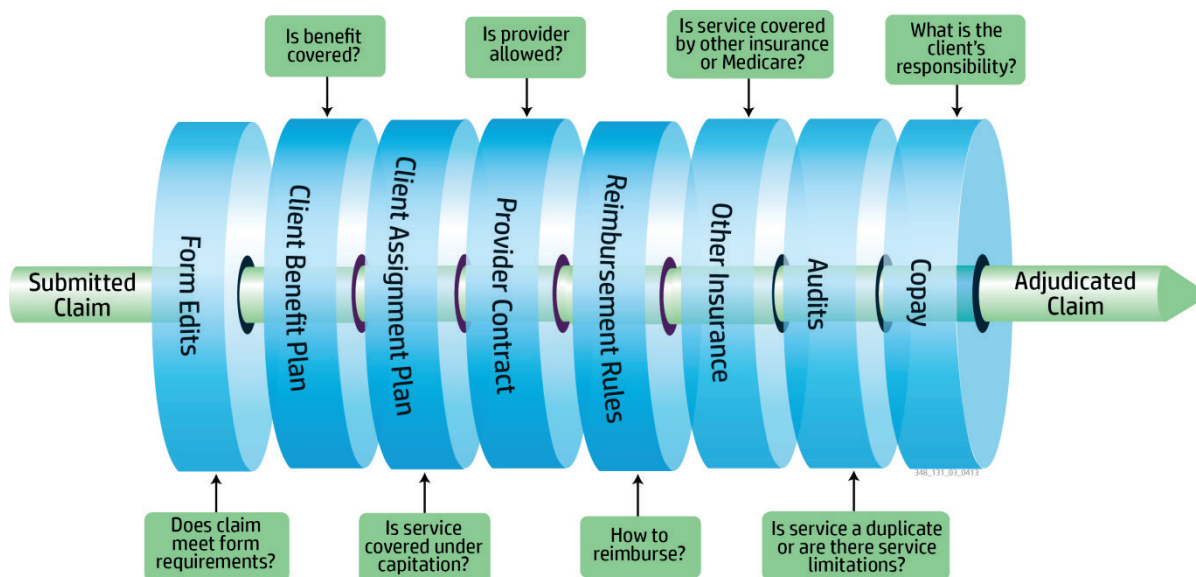
The @neTouch family of features within the interChange UI contains enhancements that go beyond the basic MMIS UI. These are user personalization and navigation features designed by users for users.

HP is proud of @neTouch. It adds value to front-line staff members, which will add value to the Department. Efficiency and effectiveness are increased across the board.

How BPA Works

The interChange BPA process and rules allow the policy and claims to be configurable end to end. The following figure is another representation of how the claim will move through these rules and shows end-to-end configuration of the process.

How Rules Are Applied to a Claim



interChange BPA uses a business rules engine to deliver a user-configurable, faster, and more responsive system to manage benefit services and program features. User-friendly, online MMIS browser pages allow the configuration of benefit plan criteria, edit or audit disposition rules, procedure, drug, diagnosis, diagnosis-related group (DRG), and revenue code rules and restrictions, and the establishment of pricing rates and methodologies. interChange presents users with a graphical interface displaying a combination of easily understood parameters and navigation paths. Parameters can be combined in numerous ways through online browser screens to establish a flexible, yet structured, rule repository, as the following figure highlights.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

The BPA methodology keeps simple tasks easy. Step-by-step processes prevent erroneous rules and keep long-term defined policy clean and accurate. interChange BPA uses the business rules engine to deliver a configurable, faster, and more responsive system. Rules help policy analysts and SMEs define and manage how services are covered, delivered, and processed.

Another important feature is rules traceability. The system keeps track of which rules have been applied to the claim and how they processed or set. Even further, the system allows users to quickly trace that path from the claim, to the rule, to the benefit plan attribute, to the pricing and reference information. This allows for quick research and understanding of what the system and process is doing and how it affected the transaction. The following figure shows the portion of this process linking the claim to the rule.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

The right processing rules allow the following actions:

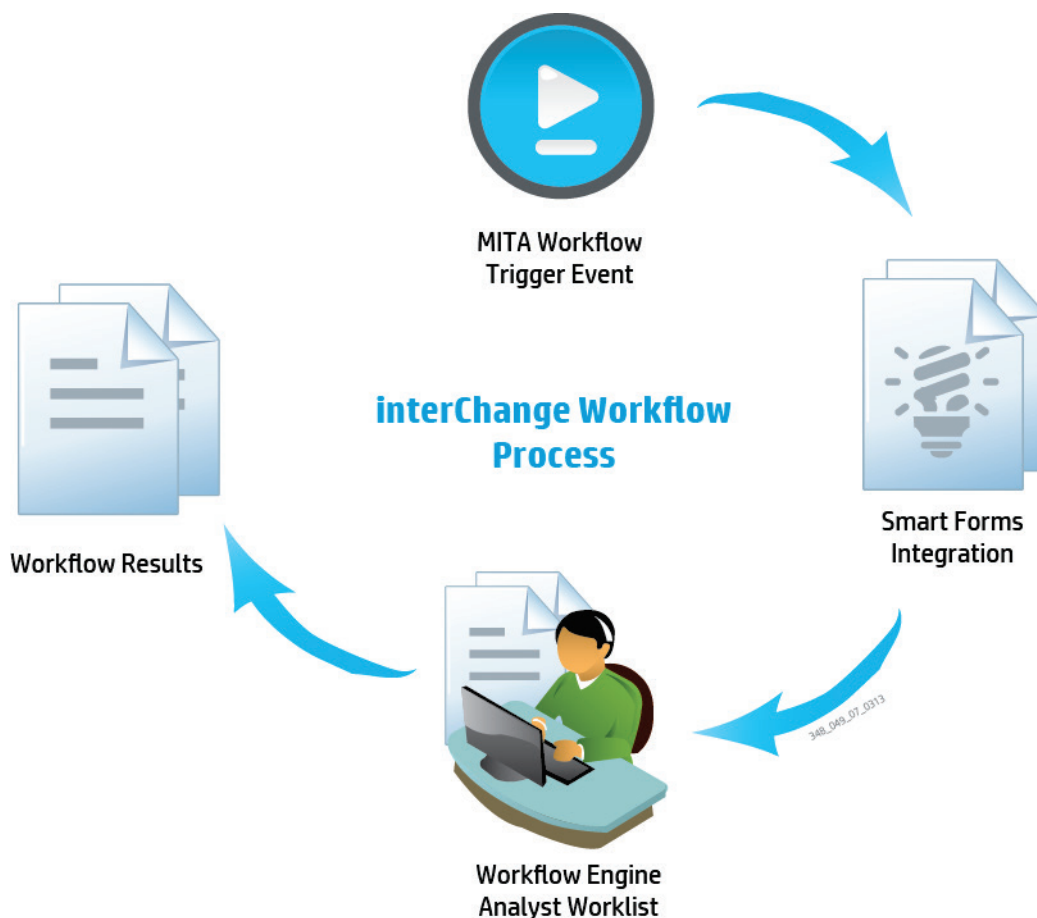
- The Department can identify, refine, and maintain the business rules needed to manage today's Medicaid healthcare requirements.
- The Department can logically group services according to recognized medical standards and incorporate rules at any level within the classification.
- The Department can configure its rules according to the way its policies are written—as broadly or with as much granularity as needed.

interChange BPA uses rules management to define and manage how services are covered, delivered, and processed. The business rules engine adds value to support healthcare services management through interChange easily and effectively. BPA provides an efficient structured process for managing complex healthcare policies and responding to the need for rapid reaction to legislative changes.

Enhanced Response to Business Changes

The business activity monitor reports the inflows and outflows. As business changes occur, it is easy to spot bottlenecks or other increasing needs. This allows the Department to quickly readjust the business workflow to accommodate either an increased load or modification to smooth out the flows.

interChange Workflow Process



Many functions can be implemented as an end-to-end business process using workflow and the rules engine to automatically flow items for an immediate decision. The ability of the portal to upload documents directly also will facilitate the business review. The information needed for a decision is brought together in the workflow. A good example of this process is the online application process. For the provider application, the questions are organized around the provider type and specialty, and whether it is a group or individual practice.

The ability to closely monitor the workflow and make rapid adjustments will enable the Department to service more clients with the same levels of staff and resources. The portals are designed to provide and facilitate direct interactive service by clients on the web. The system also provides a quick feedback to the clients through email or correspondence and even shares them to direct contact from staff members. The system has been designed to route the

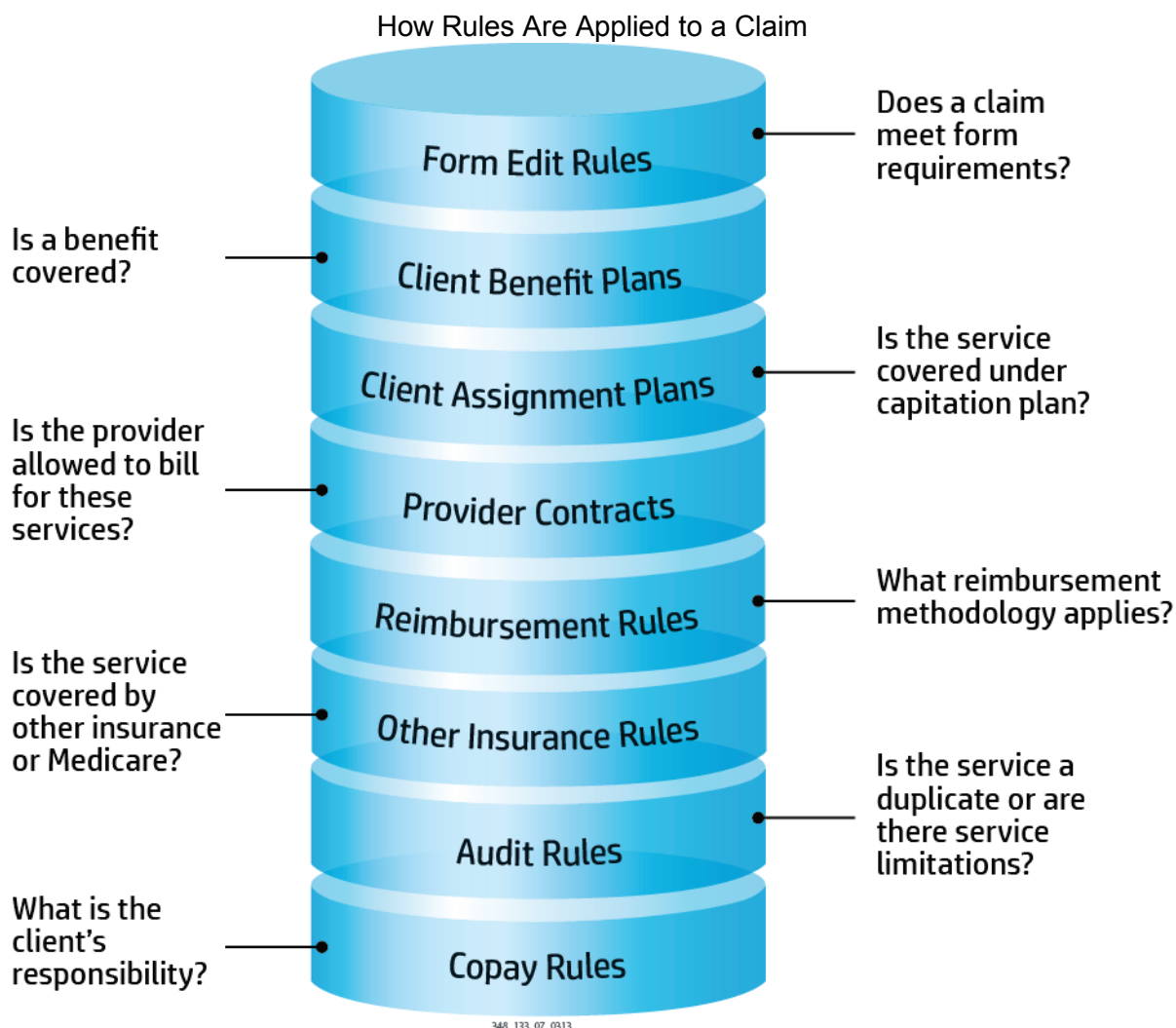
information to the stakeholder who is using the portal or to the business staff member who must complete a service.

More Efficient Business Rules and Business Processes Changes

The HP Colorado interChange solution, using the BPA and the workflow, saves time by allowing the business staff members to make changes directly. The rules engine uses GUI-based intuitive screens that facilitate quick entry with minimal keystrokes. The workflow provides consistency checking and some capability for simulation to facilitate the validation and verification of the process change. We detail workflow for screen images and rule entry in RESPONSE 38m.

With a few entries, the BPA rules engine can implement policy quickly by the business staff, thereby eliminating coding and process around a code change. Changes are quickly made and easily tested at the business staff level. This means the time to implementation is short and the total outlay of resources compared to a code change is greatly reduced. Also, the overall accuracy is much better because the code components of the rules engine are fully tested and validated.

The following figure highlights the gamut of rules maintained as part of the BPA.



The MMIS is designed to make changes through tables, workflow processes, and the rules engine. These are easily entered directly by the business personnel. Real-time reporting through the Business Activity Monitoring (BAM) allows quick detection of out-of-control or increased load situations. The workflows can quickly be adjusted to handle the situation that is causing the load.

Because required coding would be small, the change can be done quickly and directly by business staff members, minimizing the effect of change as code modules are not affected. This also minimizes the effect to other preexisting processes for the same reason. This will make the cost of change much smaller.

New Technology Integration

The architecture is designed to add new services by connecting them through the ESB and exposing only the services. The web services and workflow then coordinate the calling of these services with the preexisting services. The coordination is done at the business layer and not the

code level, so the changes in the layers are separated from each other. It is easy to add new services or replace or upgrade the technology of a service itself. For instance, if we need to upgrade a shared service, we change the technology and the replaced service connects with the same business interface as before. The following figure shows how the business layer isolates the technology layer (applications) from the stakeholders.

The network figure shows how the technical services (in green) and business processes (in blue) are connected through the ESB. In this case, an activity can use several services to obtain information and consolidate several other services to actually perform an update or complete an inquiry. The rules engine can verify that the selected data meets the requirement or policy for an update and then return the information and status by the data access service to the calling business request. In this case, we may do the update depending on the result from the business rule. The logic and connections to satisfy the service request are in the business layer.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

The technology is in the application layers (green boxes) and represents the individual COTS shared services or MMIS services such as claims, TPL, or reference. The blue boxes are the business services and are defined in terms of business logic flows and vocabulary. Change at the technology level has no effect on the business layer and vice versa.

Longer System Life Span

The following specific aspects of the interChange MMIS deliver a solution that lengthens the effectiveness and value of the MMIS:

- interChange Connections and the web services provide the ability to perform service integration across the healthcare ecosystem and among components in the MMIS.
- interChange BPA enables broad control and flexibility across business rules used to process transactions.

- interChange Workflow enables workflows to adjust throughout the contract to the business processes needed to effectively manage the business.
- The COTS tools are service-enabled and (through interChange Connections) can become plug and play, delivering business effectiveness for aspects such as correspondence and document management.

HP designed this solution that uses state-of-the-art COTS solutions for the shared services and an MMIS that is installed in 13 states. The COTS products are supported by vendors who continually maintain the product across technology and application. The vendors provide a path for updates that minimizes impact to their installed base.

The MMIS uses web services and an ESB to connect services or functions, which minimizes organizational disruption because the customer business services and business information formats remain the same. The configuration control processes are designed to manage change and minimize the effect on the organization. Configuration control comprises identifying the effect and providing the change in a project managed environment where the components are well tested before moving to the next level. The development methodology is highly structured and integrated with the stakeholders, thereby eliminating surprises.

The MMIS components are. NET, C, Oracle database, Autosys, VMware, and other proven vendor components or products. HP follows standards of good practice around code implementation and the operational practices. In the case of vendor components, we maintain the releases at levels that have product support. This minimizes issues to the stakeholders and provides a technology that is supported by a larger community. This promotes a longer system life and provides a body of knowledge and practice that minimizes disruption to the customer through various upgrade and modification cycles.

Appendix A Technical Requirements

The functions and processes that follow support the business areas and are designed to protect and maintain the data and applications necessary for ongoing operations, efficiencies, performance, and quality control.

Systems Interfaces

HP will use the ESB and the B2B adaptors as part of an interface manager. We will define each interface and the elements necessary for sending or receiving. HP works with stakeholders on each side of the transaction to verify there is agreement on the data definitions, transaction mode, frequency, and other pertinent information to support a smooth transfer of information. interChange comes with standard interfaces for CMS, healthcare transactions sets related to eligibility, claims, payments, coordinated benefits (COBA), and Meaning User Module–related interfaces.

Our 13 interChange implementations have given us experience in connecting with state eligibility systems, BIDEEM systems, and even different PBMSs. We detail the individual Colorado interfaces and our approach to them in RESPONSE 38k.

Systems Performance

The HP solution has been designed to provide uninterrupted service, other than scheduled downtime. HP uses a combination of hardware and software components to provide failover if a component failure occurs, such as a server or a network. Storage uses RAID6 to manage media failure. HP also provides an alternate disaster recovery site in Colorado, should the primary site become unavailable.

The component hardware and software systems are set up with warnings and alerts to anticipate issues or bottlenecks before they cause problems. These are monitored by experts who will attend to the notifications in the following ways:

- Application cycle monitors verify that business cycles are completed on schedule and correctly.
- System administrators validate server resources are working and sufficient to support traffic.
- Database administrators monitor database traffic and load.
- Network administrators monitor load and bandwidth.

The load balancer and the number of ESX servers are set up so that responses meet the required transaction times. We use Oracle RAC so that a failure of a single database server is taken over by another. BAM provides a real-time view of the business operations and allows monitoring of their performance by the Department and the account Business Operations team.

We detail the performance requirements in RESPONSE 38p and Appendix A – Requirements and Performance Standards Matrix.

Infrastructure

The Colorado interChange infrastructure will include the facility, servers, network, and security infrastructure around edges, networks, server access, and data transport modes. These are monitored 24 x 7 and have been set up with alerts and notifications. Anything that is unusual or is reaching a resource limit—such as bandwidth, CPU, or storage—will trigger an alert that will be addressed. The HP team uses the HP SiteScope and the HP SRA to monitor and collect data. The data is used for planning and for provisioning additional resources to meet growth or service-level agreements (SLAs). Some high-level measures are included in the inSight Dashboard around call volumes, through-put, and uptime. Although the Infrastructure team likes the grainy technical level, the inSight Dashboard is geared toward updating the Department using business terminology and artifacts.

Workflow Management

Workflow technology will transform almost every facet of the daily work with the MMIS. It is one of the key areas of transformation requested within this RFP. HP uses the inSight Dashboard to monitor performance of the business processes. We offer further detail of the workflow itself in RESPONSE 38p and Appendix A – Requirements and Performance Standards Matrix.

What gets measured gets done, and this straightforward approach is exactly the philosophy behind the interChange production reporting environment, specifically the capturing and reporting of key performance indicators (KPI). HP's solution is a comprehensive system and services metrics approach that provides unprecedented access and visualization of efficiency and effectiveness of these metrics, which in turn reflect the quality of the services provided.

inSight Dashboard Defined

The interChange workflow engine has the ability to capture detailed metrics, including start and finish date and times and the responsible party for the business action taken on every step of a workflow. The interChange workflow engine enables users to evaluate the efficiency of each business step, the overall efficiency of the MITA business process, and how effectively each analyst is in accomplishing the work. Such detailed, accurate, and easy-to-evaluate reporting is inherent within our solution, and we developed it with the CMS vision of continual evaluation and MITA process efficiency across time.

How inSight Dashboard Will Benefit the Department

Besides the business process flow metrics reported through the workflow engine, our Colorado interChange solution includes the interChange inSight KPI Dashboard, where the key metrics that are aligned to service delivery excellence are captured and reported. The HP solution exceeds expectations by going beyond static dashboard presentation to enable users to have a true analysis tool at their desktop to evaluate, drill into the details, and filter the metrics to better understand the business drivers behind the KPI numbers. We provide our inSight Dashboard through a centralized content management system of Microsoft SharePoint. Through the inSight KPI Dashboard, the technical and operations performance data is directly available to the Department and HP leadership team for real-time, meaningful analytics.

How the inSight Dashboard Works

With the HP inSight KPI Dashboard, what gets measured gets done correctly. The HP Colorado interChange solution is a forward-looking approach that directly aligns with the MITA vision of continual measurement and improvement across time.

To further demonstrate the advantages of the interChange inSight KPI Dashboard, we provide the following example.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

Within this contact management example, the many advantages of the interChange solution become apparent. First, the top half of the screen lists the many interactive dimensions that the reviewer has access to, such as “Frequency Description, Contact Date, Contact Reason Description, and Contact Method Description.” The manager can change these dashboard filters to drill into the specific metrics they desire. The exciting part of this process is that by changing the filters, the reporting displays of the dashboard change dynamically. Users do not need to rerun a report and wait for a response—the presentation of the results is completed in real time—making the interChange inSight KPI Dashboard more than a reporting tool. The bottom half of the screen shows historical data. In the multi-presentation method illustrated in the previous figure, line charts—complemented by the two pie charts—provide quick and visually meaningful information. Users can change the view if desired, as the following figure illustrates.

The K2 package also supplies workflow management tools. The following figures are examples from the workflow section of the RFP response.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**



The preceding and ensuing figures depict the process overview report that drills down into a single workflow instance. The report details the statistics such as completion time for each step of the workflow process. The reports display the productivity statistics associated with an individual step in a workflow process or a user. Managers can use this information to determine easily which workflow steps may be a roadblock in business processes and update to increase efficiency.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

Managers also can identify individuals who may need additional training or support to complete certain steps in the workflow. Users may drill down into key data and customize reports providing ad hoc information to aid in business process management, as the following figure details.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

Alerts

Using the dashboard gives the Department another key feature: alerts. HP can configure alerts within the system so that monitoring occurs in the tool and dynamically informs management of changes that go beyond the intended range. This allows users to then be alerted to go research further and address potential concerns. The dashboard enables Department users to quickly view status and understand program direction. The alerts take this to the next step, indicating the potential locations to address and when.

The inSight Dashboard offers access to performance indicators like never before. HP adds value to the Department's ability to be responsive and proactive.

Desktop Publishing and Content Management (Electronic Document Management)

The current business processes of reviewing, revising, and obtaining approval of content published—such as provider manuals and bulletins—are largely managed at the desktop involving passing documents from person to person by email. This slow, loosely managed approach provides little visibility into status and metrics. The content management solution features in the new HP Colorado interChange solution provides an innovative solution using COTS tools and workflow to transform this process through the consistent application of policy, clear audit trails, and reliable, consistent outcomes.

SharePoint is the perfect application to handle the diversity of content produced to support the MMIS and program. It is integrated into the larger interChange architecture through Business Services and Connections and shares the same underlying workflow technology as the Core MMIS. The following sections will introduce the benefits of our solution for Colorado and its alignment to CMS 7SC and stated Colorado goals.

The following figure presents the new approach to content management.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**



The Colorado Medicaid program will benefit in several ways from the implementation of the HP content management solution:

- SharePoint, a browser-based application, is easy to access, maintain, and use.
- SharePoint is an intuitive application requiring little user training.
- Out of the box, SharePoint administrators can create document libraries, nested sites, tasks, wikis, calendars, and more. This gives the teams many choices for collaboration, documentation, communication, and tracking.

- Built on the .NET framework, SharePoint will easily integrate with the Colorado interChange through the interChange Business Services Framework and Connections (BizTalk ESB).
- K2 blackpearl workflow for SharePoint is a COTS product that brings powerful, visual workflow capabilities to content management. For example, K2's ViewFlow offers a graphical representation of current workflow processes displaying possible paths and steps already taken. Workflow is part of the interChange Business Services Framework, enabling standardized workflows throughout the MMIS.

Data Management

Accurate data is the cornerstone of healthcare management solution. HP is aware of the critical role that the MMIS has in terms of data management. From performing highly efficient transactions using the MMIS data stores to supplying Medicaid reporting data marts and the delivery of data to the BIDM, the Colorado interChange has the data management approach that best meets the Department's needs. The HP FTS tool is used by business managers to manage the performance of interoperability of the data transfers between the MMIS and other stakeholders. As we learned through working with our Florida customer, we managed the data that needed to be sent to and from a PBMS vendor and still performed the drug rebate processing and maintained a claim history.

We provide additional detail for data management, especially around security, in Appendix A – Requirements and Performance Standards Matrix and RESPONSE 38n. The sections that follow detail the data management and metadata management infrastructure and processes.

The HP Colorado interChange MMIS provides the following features:

- A solution that facilitates the secure transfer of provider, client, claims, and other related information to the BIDM according to industry-standard extract, transform and load (ETL) processes. We will work with the Department and the BIDM vendor to define and support the appropriate data exchanges and data governance structures.
- Normalized logical and physical transactional data structures that reduce the redundancy of data, keeping data management tight and quality high and making long-term data management easier and more accurate.
- Data marts that are specifically designed to facilitate interactive online management reporting and the inSight dashboard reporting of KPMs.
- An ad hoc data store that provides the ability for fast MMIS ad hoc reporting of the most common data attributes used to manage the business.
- Accurate and timely data to the BIDM using data transfers that the ESB manages, providing a quality audit trail of the data management activities.

HP will work with the Department in meeting its requirements.



The system simplifies data management for the providers and trading partners through interoperability with the MMIS. Our HP Healthcare Portal and interChange Connections ESB/EDI solution will help the Department meet many of CMS' 7SC and advance in MITA maturity through the following features:

- **Modularity standard—different media formats**—The interChange Connections, combined with workflow, web applications, SOA services, and event messaging, support human and automated business process steps.
- **Reporting and business results conditions—monitor SLA/KPI**—The interChange interactive reports and the inSight Dashboard provide unparalleled transparency to KPMs.
- **Interoperability condition—data sharing**—The interChange Connections solution simplifies sharing of standard transaction sets with trading partners and the enterprise data warehouse through an integrated ESB, FTS, and service monitoring framework.

Information Architecture and Data Modeling

The HP Colorado interChange provides the established logical and physical data models, data governance, and overall data architecture that maximize transaction processing for the business features. Our approach supports HIPAA data standards and interoperability through the Connections ESB/EDI capabilities. The solution also contains the ability to properly manage the data and provide timely MMIS ad hoc reporting and excellent support of data extraction to the BIDM. The following table summarizes how the Colorado interChange solidly addresses the requirements.

Data Management Solution Advantages

Data Management Requirements	Colorado interChange Data Management Solution
Data Governance	Our SDLC and complementary change management tools control the approved data changes within each environment. This governance provides the foundation for defining and modifying the data exchange standards across time.
Data Architecture	Tuned relational database configured at a third of the regular level optimizes data access versus data redundancy. This uses online transaction processing (OLTP) architecture for operational transaction processing and online analytical processing (OLAP) architecture data marts for high-speed ad hoc support.

Data Management Requirements	Colorado interChange Data Management Solution
Data Sharing Architecture	Access to data is strictly controlled through data access objects and data factories. This control protects data from unsecure access and enforces a pure n-tier architectural layering. It also provides a framework for secure data exchanges across the ESB by providing an additional layer of control and security to data access activities.
Conceptual Data Model	Optimized for healthcare across 40 years, related data is grouped into business areas that map to MITA through standardized naming conventions.
Logical Data Model	Highly optimized COTS data modeling tools render the logical data model into the physical data model for precise change management control.
Data Standards	Tools fully support industry-standard HIPAA transaction sets.
Manage Information	Advanced interoperability is available through the Connections ESB.
Electronic Data Warehouse Support	Informatica, a top-ranked ETL tool, supports efficient MMIS data extraction to the Department's data warehouse.

Our extensive experience in supporting MMISs has enabled us to recognize and incorporate five principles in successfully implementing, using, and controlling data management:

- Adherence to and active participation in the development and implementation of industry standards and guidelines
- Approach to data management from a database perspective
- Approach to data management from an infrastructure perspective
- Approach to data management from a data element perspective
- Approach to data management with stakeholders of the MMIS in mind

The Colorado interChange meets the applicable standards and guidelines related to data management directly. This capability is a fundamental reason interChange has been CMS-certified in 12 previous implementations, with another pending.

HP uses best practices learned from more than three decades of Medicaid program support and guidance from industry organizations and CMS. CMS' guidance for developing an MMIS and the requirements put forth by the Department require a solution that provides the necessary flexibility and agility provided by an SOA. Part of the MITA initiative, this direction moves a Medicaid enterprise from a traditional, subsystem-based MMIS to web-based, client-centric

systems that are interoperable within and across levels of government and provide easier, standardized ways to manage data.



Our solution provides an enterprise-level data exchange, data cleansing, data store, and professional data-rendering capability. We support and use data standards to improve the long-term cost-effectiveness of MMIS support and development. The use of data standards promotes data consistency across the State healthcare enterprise, including the BIDM. Through integration of COTS software solutions, we can reuse standard business features throughout the solution. HP reviews national standards for data exchange and open standards for technical solutions. Our architects will use the healthcare standards and determine how to adapt to them, as they evolve across time.

Besides the requirements set forth by MITA, our proven solution for Colorado is adaptable to support various government mandates such as the American Recovery and Reinvestment Act (ARRA), Health for Economic and Clinical Health Act (HITECH), and the ACA. Through the progression of interChange MMIS development, HP adapts to changing industry data standards—such as ICD-10 code sets and the ACA Operating Rules—demonstrating the ability to develop technology to meet maturing business needs.

As the largest government healthcare processor in the nation, HP fully supports and is actively involved in the development and implementation of the accepted healthcare standards, including HIPAA. This involvement includes data, transaction, privacy, and security standards. We take these standards into account as we design our systems and implement customer-driven requirements. HP participates heavily in many standards groups, including ANSI Accredited Standards Committee (ASC) X12, National Council for Prescription Drug Programs (NCPDP), Health Level 7 International (HL7), Nationwide Health Information Network (NwHIN), and Council for Affordable Quality Healthcare (CAQH). We bring these standards into our development processes and customer communications to verify that our systems continually evolve to support the changes in these standards as they occur.

The Colorado interChange will use the interChange Connections for EDI processing data exchanges. The communication between the MMIS and its stakeholders—such as clients, providers, the Department, and other State agencies—is controlled through our standardized data management data exchange process using ESB Connections.

HP bases our security features on national security standards for security levels and privacy markings. Security guides and declassification rules can be set in accordance with Chapter 3 of Department of Defense (DoD) standard 5015.2 v3.

Data Management Tools

HP proposes various software tools to support data management of the Colorado interChange. We identify these tools in the following table.

Benefits of Software Tools for Data Management

COTS Software Tool	Data Management Support Role	Benefits of Data Management Software Tool
CA Technologies Erwin	Data modeling	Provides the ability to model data across the MMIS enterprise into a series of data stores and data marts. The data marts form the basis for the MAR online reporting and inSight metric dashboard solution.
Informatica's Data Explorer	Data profiling	This scalable high-performance software tool is used for accessing and integrating data from virtually any business system, in any format, and delivering that data throughout the enterprise. This tool will be used during the DDI Phase to facilitate the data profiling activities.
Informatica PowerCenter	Metadata management ETL tool Data integration	This COTS product provides a highly scalable, highly available, high-performance software for accessing and integrating data from virtually any business system, in any format, and delivering that data throughout the enterprise. Data can be structured, unstructured, and semistructured. It can be from a relational, mainframe, file, and standards-based data source. Used for ETL processes (such as during data conversion), event-based change data capture, and to keep the Colorado interChange in sync during DDI.
Microsoft BizTalk	ESB	This product is a market leader that is designed to connect, mediate, and manage interactions among heterogeneous services and multiple ESB instances across an enterprisewide service network.
Oracle	Data diagnosis and tuning	Oracle offers a comprehensive set of automatic performance diagnostics and monitoring features built into a core database engine and Oracle Enterprise Manager. This automates the entire application-tuning process and achieves enhancements of SQL performance through real-time monitoring and SQL advisers who are integrated with the Oracle Enterprise Manager.
Oracle RDBMS	Data repository	HP has a history of success using the Oracle relational database in many Medicaid states. We will continue this database model that directly maps to the architectural principles of scalability and security for the Colorado interChange.
SAP BusinessObjects	Reporting	BusinessObjects supports the generation of certain claims, provider, and customer ad hoc reporting. The advanced search

COTS Software Tool	Data Management Support Role	Benefits of Data Management Software Tool
inSight Dashboard and SharePoint (Microsoft) K2 BAM (K2 blackpearl)		capabilities in the BusinessObjects reporting repository are robust. The search lets users restrict or expand the search to various folders and search by content types or report fields such as title, description, and owner. inSight Dashboard allows dashboard servlets to run in real time on SharePoint. The BAM product from K2 collects and displays real-time activity in charts and other dashboard representations.

Data Management from a Database Perspective

One significant advantage of our solution is its foundation on the CMS-certified Wisconsin interChange MMIS and its associated data model and data services. This solution is not ground-up development or a first attempt at a transfer; but a proven, stable environment and architecture. The data and application layers are distinct. HP interChange provides Colorado with a proven data model that includes the OLTP model for high-performance transactional processing for our claims engine and OLAP for effective MMIS ad hoc reporting. Under the OLAP structure, the data is organized to support fast and accurate reporting. The interChange MMIS data structures have been continuously refined and improved through HP implementations for other states in support of Medicaid healthcare business services. This refinement reduces risk for the Department because the core of the solution is fully functioning and certified in other states, rather than a conceptual, unproven design.

Our solution uses the Informatica PowerCenter products to retrieve data using custom ETL processes to transfer data to other stakeholders, such as the data warehouse vendor, supporting a MITA-aligned logical data model. The software products are scalable to support large data volumes and meet enterprise needs regarding security and performance. These products provide guidance for data governance and data migration.

HP's use of Oracle software provides a data replication feature to synchronize the primary core MMIS and backup system data through rapid update of transactions to the backup data center's failover environment. This approach provides a level of comfort that access to data and critical systems is available continually—except for scheduled downtime. Also available with the Oracle RDBMS is the product's inherent tightening of data quality compared to former MMISs. Additionally, our proposed solution performs field-level editing during updates and auditing of updates made through the user interface to achieve consistent data quality for the Department.

We will use CA ERwin to maintain the definition of the Oracle database table structures and table relationships. Our change control processes will compare differences between the data

models and the Oracle databases and generate accurate SQL to promote table changes to the Oracle databases, allowing additional new data elements to the system with minimal effort.

Data Management at the Infrastructure Level

The Colorado interChange provides efficient and secure infrastructure for the data management of the solution. We have established industry best practices, and the infrastructure data management solution prepared for the Department is based on the lessons learned from several MMIS implementations.

Support for Multiple Evolving Data Interfaces



From an infrastructure perspective, the HP focus on data includes data received and transmitted to the MMIS and data at rest or in storage. For data received or transmitted to the MMIS, HP's Connections ESB/EDI capabilities provide readily available channels for secure HIPAA transactions and other data exchanges. These channels are supported through a HIPAA-compliant system developed with a three-tier architecture model. This architecture separates external communication, application, and data layers. Reliability and performance are the foundational concerns of a SOA infrastructure built to deliver high-availability, fault-tolerant, and highly secure EDI services. It supports numerous communication protocols, file types, and integration capabilities. It can quickly integrate, manage, and automate dynamic business processes by exchanging business data and documents among applications, within or across organizational boundaries.

Support for Continual Data Security and Encryption

Additionally, electronic PHI data is protected by electronic security measures and HIPAA-compliant business processes. We understand data of this nature and prevent the data from being altered during transmission by enforcing secure delivery and limiting the role-based access to the data. Data at rest or stored on servers within the HP network is encrypted in the HP storage area network (SAN). Desktops and laptops are data encrypted with McAfee Endpoint Encryption. Data in motion are encrypted with HP network appliances and will traverse the wide area network (WAN) inside IPSEC encryption tunnels. Access points to send or retrieve data in the MMIS will be guarded by the use of IPS/IDS devices and firewalls. HP uses tape encryption for the data stored on tapes on-site and off-site and applies appropriate rotation and retention periods.

Support for Ongoing Data Availability

Our focus on data management is on the content of the data we are processing and how the Colorado interChange is handling the data. Our proposed solution has software that collects data on usage and other statistics including application servers, database servers, CPU, memory, and SAN space. This information is used for short-term performance objectives to protect system availability and aid in planning for enhancements and longer-term capacity. The SOA ESB has diagnostic and measurement tools that collect statistics on load, time, and transaction volumes. The database diagnostic packages also collect database performance statistics that includes CPU,

SQL performance, number of users, and type of activity. This data is collected regularly and retained for near-term analysis or historical review.

The HP SiteScope tool is used to measure transaction times at the transaction level and also retains historical information for later review. Subsystem load also is reviewed based on the business processes such as claims processed, eligibility transactions, and other business-related variables. This type of information is used for planning, tuning, and staffing. The goal of these data management tools and processes is to produce a continual optimization of data availability.

The Colorado interChange will operate on a mission-critical platform of HP Superdome systems. This solution provides virtualization that enables the dynamic provisioning and management of resources to adjust to fluctuations in the business workloads, shifts in business strategies, and changes in the MMIS data load. Virtualization also supports system infrastructure management through a single console and provides the ability to automatically provision or save work images for rapid disaster recovery.

Approach to Data Management from a Data Element Perspective

HP applies strict principals in the data information definition and management. Database administrators (DBAs) and architects manage the information model following documented procedures. These procedures guide the end-to-end process including data element naming conventions, association to the appropriate logical and physical data models, valid values, or validation algorithms. To achieve the greatest reuse and consistency, the same data element is associated with multiple data models. In this way, we can standardize the definition of the billing provider, making it the same in the various business areas, such as provider, claims, or care management. This approach reduces data redundancy and allows better change management across time.

Our data management process also establishes and manages the metadata related to the data including objectives, sources, types, references, and relationship to standards. The data element dictionary is defined and maintained in ERwin and published in HP PPM. The information for the Data Element Dictionary (DED) is pulled in real time and the DED is updated as the data elements change, so the DED is always a current reflection of the system and no secondary documentation maintenance is required.

Our DBAs have years of experience using the ERwin Model Mart and can quickly add new data elements and tables to the new Colorado interChange as enhancements are made. The DBA configuration management tools allow the logical data model in ERwin to be realized as the physical data model within Oracle as part of a controlled SDLC deployment methodology.

Additionally, Informatica's Data Explorer will be used for data profiling as part of the conversion. These tools, along with market-leading database products, allow HP to create a data infrastructure that is easily configurable and role-based with continual access to data—excluding scheduled system maintenance time. The definition of data ownership and access at the system

level enables the data arbitration protocols to be enforced. HP will meet the Department-defined data retention requirements, including access to online claims history.

Quality Management

For more than 40 years, HP has been evolving a quality management (QM) methodology that stresses early involvement of our customers and stakeholders, careful attention to our customers' needs and interests, and precise application of strong standards. Through this comprehensive QM program, HP delivers meaningful monitoring and performance measurement; on-demand, iterative and flexible quality reporting; and collaborative, continuous improvement processes. In recognition of the Department's special interest in quality management, HP brings these program features in combination with robust COTS tools to provide the Colorado interChange with a best-in-class QM plan.



HP has demonstrated the QM approach on many projects, including multiple interChange implementations. Although our approach begins with our methodology and standards, HP will customize it for the Colorado interChange environment. We incorporate process knowledge and lessons learned from previous implementations. Coupling the methods and processes with HP PPM provides the Department with a high degree of flexibility for QM, with a focus on the areas of specific interest. The following table describes the three focuses of QM.

QM Focus Activities

Focus	Activity
Quality Planning	Identifying quality requirements or standards and documenting how the project will demonstrate compliance, performed in parallel with the other project planning processes
Quality Assurance	Auditing the quality requirements and the results from quality control measurements to verify that appropriate quality standards and operational definitions are used; provides an umbrella for continuous process improvement, which is an iterative means for improving the quality of each process
Quality Control	Monitoring and recording results of executing the quality plan activities to assess performance and recommend necessary changes, including quality standards for project processes and product goals; identifies causes of poor process or product quality and yields recommendations to eliminate them

The QM methodology complements the Healthcare Enterprise EDGE SDLC with the application of quality improvement concepts. Beginning with the Start-Up Phase, the HP quality manager will promote communication and collaboration with the Department and the MMIS teams to support and resolve quality concerns, support relationships with the providers and provider

associations, and advocate independence in quality assessments and recommendations. The QM plan will serve as the baseline for QM principles and tasks to execute delivery of quality.

QM Plan

Reviews, audits, and testing provide the foundation for the QM plan because they provide the guidance for determining if the solution adheres to the correct standards and requirements. Reviews and audits are broken into two categories—product assurance and process assurance. Testing is broken down into multiple phases and described in full in the SDLC document. The following table describes our quality assurance reviews.

Quality Assurance Reviews

QA Review Type	QA Review Activity
Deliverable Review	Provides the framework for iterative and interactive creation, review with the Department, and delivery of contractual deliverables
Work Product Review (WPR)	<p>An internal HP process builds into the life cycle a continuous emphasis on quality toward the following:</p> <ul style="list-style-type: none"> • Identifying and correcting problems early in the life cycle because problems caught and resolved earlier cost less to fix than those caught later • Improving the quality of deliverables, thereby increasing customer satisfaction and satisfying of requirements • Reducing time and costs resulting from rework <p>Measuring the efficiency of the WPR process eliminates problems before they reach the next stage of work. The WPR captures the results of the reviews to identify future process improvements.</p>
Code Review and SOA Review	<p>Provides guidance on verifying that code meets the requirements in the repository and a checkpoint that the solution uses the interChange Business Services Framework SOA:</p> <ul style="list-style-type: none"> • Providing standardization review of business services and technical services • Providing standardization review of workflow and business rules architecture
Test Plan Review	Provides guidance for assessing adequacy and completeness of verification and validation methods defined in the test plan; helps determine adequacy of test coordination and products—such as scripts, conditions, and scenarios—to begin testing activities

QA Review Type	QA Review Activity
Post milestone project review (PMPR)	Held at defined milestones and after project to assess development activities on project and provide recommendations for appropriate actions; where applicable, includes lessons learned while building the new system
Project health check	Provides project managers and leadership with means to determine effectiveness of project management practices on their projects; includes templates to audit project to measure process maturity and strength of practices being applied
Operational readiness review (ORR)	Provides guidance for assessing project's readiness to leave Test Phase and enter Implementation Phase; includes project leads providing status on teams' readiness to support solution going live; uses deployment checklist to verify completion of deployment activities
Configuration management baseline audit	Verifies that we have baselined work products as per plan and must be completed by time specified and for scope defined in plan
Phase reviews	Includes quality reviews at end of each phase that enable HP to manage each SDLC phase of project as a discrete and identifiable stage; gathers information needed to move project forward to next phase or decision point; serves as the following: <ul style="list-style-type: none"> • Quality-control checkpoints, where quality of execution is the focus • Successful accomplishment of phase deliverables and milestones • Risks identified with mitigation plans for next phase

The reviews and monitoring provided by the QM plan verify the following:

- The software life cycle processes comply with the contract and adhere to the plans.
- The internal software engineering practices, development environment, test environment, and libraries comply with the contract.
- Applicable prime contract requirements are passed down to each subcontractor, and the subcontractor's software products satisfy applicable prime contract requirements.
- The acquirer and other parties are provided the required support and cooperation in accordance with the contract, negotiations, and plans.
- Deliverables are in accordance with established standards and procedures.
- The staff members assigned have the skills and knowledge needed to meet the requirements of the project and receive necessary training.

Continual Quality Improvement

HP quality managers will work with the Department to apply continuous, collaborative quality improvement. HP's methodology supports tools tailored to MMIS applications and functions, reduces defects and variation, and optimizes and controls process capability. The following table summarizes quality management techniques that HP can use on the Colorado interChange project.

Quality Techniques Available to Colorado interChange

Technique Type	Technique	Purpose
Generating ideas	Brainstorming	Generates multiple ideas about a problem or topic
	Cause-and-effect diagrams	Graphically helps determine causes of a particular effect
	Five Ws	Helps discover the source of a problem by asking and answering who, what, when, where, and why
Making decisions	Multivoting	Finds the important items on a list; helps prioritize and avoids a "win-lose" situation for team members using the tool
	Nominal group technique	Prioritizes items in a list and makes decisions based on inputs from each user
	Pairwise ranking	Prioritizes items in a short list and reaches decisions by consensus
	Benchmarking	Measures our progress against others and helps identify key areas for improvement
Analyzing problems and causes	Flowcharting and process mapping	Shows how the whole process works; identifies critical stages of a process
	Cause-and-effect diagram	Graphically helps determine causes of a particular effect
	Performance measures and metrics	Use of metrics and supporting measures to monitor trends and determine improvement areas
	Data analysis	Graphical and statistical, evaluates results from metrics
	Causal analysis	Approach for conducting causal analysis

HP analyzes defect statistics to determine areas for improvement. If necessary, we adjust processes, standards, or procedures to maximize testing effectiveness. After a defect or problem area is selected for further investigation, the quality managers work with the Department and

project managers to identify causes for each defect or problem and recommend correction action based on highest-priority causes.

Quality Improvement Tools

As part of the project quality monitoring and improvement process, we will continually review the schedule's progress and make adjustments to mitigate potential problems. One key aspect of our approach is the implementation of a centralized project management tool that provides the Department and HP with the information and processes needed to monitor and manage the many complex activities. HP PPM provides the following capabilities using a centralized tool:

- Managing MMIS development and its array of changes
- Tracking monitoring and managing undergoing system development changes
- Tracking enterprisewide project artifacts
- Providing a comprehensive view of project management
- Providing comprehensive reporting of contractor resources

HP PPM supports a comprehensive set of integrated project management processes used to plan, monitor, manage, and execute each of the phases in the overall SDLC. HP PPM also enables each decision-maker to have greater visibility into the “big picture”—a consolidated view of the requests, issues, risks, and work streams that are affecting the project.

The HP PPM and Quality Center tools serve as our central repository for reporting and auditing MMIS performance standards. We will use HP PPM to house and manage the configuration management process and workflow. We will use HP PPM, HP ALM, and our project management methods to implement and enforce the configuration management process. By following this controlled process, changes are defined, documented, approved, baselined, monitored, managed, and reported consistently.

HP PPM automates the SDLC workflow to enable users to track complete information and provide unified access to project data needed to support business decisions. The result is enhanced quality standards included in the SDLC and managed through an integrated tool that increases the Department oversight, control, and decision-making ability.

HP ALM and SharePoint are the requirements repository that maintains bidirectional traceability between high-level business requirements, the detailed product requirements, and the various analyses, design, build, and test components throughout the stages of a project. This tool offers a framework for managing a project's end-to-end requirements traceability and provides critical functions that are integral to the success of a project, such as offering visibility and traceability between requirements, tests, and defects across releases and cycles. The HP QM team will track, monitor, and collect data using Microsoft Quality Management Progress Report, identifying quality issues throughout each MMIS phase. The HP QM team monitors and reports on program performance across the MMIS operations.

With these tools, the HP PPM will track and monitor the following items highlighted in the project status reports and status meetings:

- Major SDLC tasks
- Deliverables
- Milestones
- Resources
- Dependencies
- Critical tasks
- Major issues with action plans
- Major risks with mitigation plans

Scope verification activity is closely associated with the HP QM and controls. It is a major component of the phase reviews and serves as quality control checkpoints, where quality of execution is the focus. Effective phase reviews are central to the success of a fast-paced software development project. These reviews serve as the notice to proceed and provide the path forward for the next stage of the process along with the resource commitments.

Change Management Process

HP will establish a formal change management process following contract award to address requested changes to requirements. The full change management process has many components, such as requirements traceability, application change control, and scope management.

HP provides a sample Change Management Plan in the Examples of Previous Deliverables tab. The formal change management plan has numerous elements including the project management connected with a scope change plan appendix.

RESPONSE 38k

7.12 – System Interface Requirements	In Production? YES/NO
Description Addresses Requirements (Provide the range as applicable): 1154, 1157, 1164, 1166, 1215, 1248, 1249, 1250, 1256, 1258, 1262, 1465, 1466, 1517, 1520, 1600, 1626, 1649, 1666, 1707-1709, 1718, 1723, 1744, 1754, 1761, 1764, 1774, 1846, 1848, 1849, 1853, 1874	YES

When identifying aspects of the interChange MMIS as “In Production,” we employed a conservative approach. We identified several elements of the solution as not in production even while aspects of those components have been running in production in multiple states for years.

For example, the components comprised by interChange Connections have been in production in multiple states for a multiple years, but the expansion of BizTalk to work as the enterprise service bus is a new aspect of that offering. The interChange MMIS has performed service management for more than a decade; it is now taking service management to the next level through the ESB. Other items such as the supply of data to the BIDM vendor is listed as not in production because the specific vendor has not been selected as of yet the exact data exchange layouts have not been determined.

The interChange MMIS, as its name implies, is about change—or continual evolution as Medicaid Information Technology Architecture (MITA) envisions it. The proposed Colorado interChange MMIS is a production-proven application that has been certified by the latest CMS checklist. It is that core that is shared for the Department’s benefit and enhanced through the proposed architecture improvements

Why the HP Approach Is the Best Solution for the Department

Interfaces really are about establishing and maintaining relationships. That is why having our background and processes in state health programs is so important. Besides understanding the hundreds of traditional interfaces that are part of the full-featured MMIS ecosystem, the new MMIS can effectively interface with the modular BDIM and pharmacy vendors. This interaction takes two forms—the ability to supply the detailed data to the vendor performing those business functions, and the ability to accept outputs back into the MMIS.




CLICK FOR VIDEO

A video demonstration of the scenario Change Interfaces for New Financial Management System is included in RESPONSE 45.

The following details how the HP approach to interfaces is the best solution for the Department:

- Our knowledge of how to establish relationships with the entities that engage with the MMIS
- Our interoperability module interChange Connections that coordinates the configuration and management of interfaces

We have worked with the external stakeholders in many other states. Our established approach is a detailed, multifaceted program.

 Besides HP's interface knowledge, our interChange Connections module provides the perfect interface management solution. Connections is a module where we configure the interface handling rules for the interoperability interfaces coming into or out of the MMIS. This centralized, secure, and managed module not only processes the interfaces, but also provides transparency into the actions taken. While many other MMISs require a technical resource to investigate and research the status of the interface, through interChange Connections, the business managers have direct insight into the interface processing and their respective status. This allows business leaders to perform their own research, saves time, and immediately provides the needed information.

Meets Department Objectives and Goals

The Department's goals and objectives supported by our Colorado interChange interface solution comprise the following:

- Provides data support of automated federal reporting (financial and statistical). Where required, this provides an interface with federal systems for simplified and automated reporting and data sharing.
- The interChange MMIS has the capacity to easily interface with future EHR or PHR, HIX, HIE, and other exchange data services systems the Department may implement.
- Our solution determines and develops web-based services, and portal access, as mutually agreed with the Department for the interoperability requirements of its domain systems.
- Agency network interface—Complies with agency computer application and network security policies—such as Active Directory authentication, data encryption, and bandwidth—and provides for data interchange with other registries, agency data warehouses, and other forms of State domain information.
- Our solution accommodates electronic signatures.

With the experience of many MMIS implementations and continued operations support, interChange has been developed with the flexibility to address current and future interface requirements. Multiple transaction formats such as X12, NCPDP, and proprietary formats are routinely and successfully exchanged in states where the interChange solution has been implemented. The interChange Connections module of the interChange MMIS will accommodate the exchange of data with internal and external entities using the appropriate

media for each exchange. With our focus on The Health Insurance Portability and Accountability Act (HIPAA) security and data protection rules, HP has successfully developed and operates web-based interface applications in which providers can securely upload and download files to allow operations staff members to initiate a secure file exchange with Centers for Medicare & Medicaid Services (CMS).

To determine the best approach, HP focuses on the best solution for each interface requested by the Department. Some interfaces—such as the standard CMS, X12, and NCPDP exchanges—will require minimal Department input as HP has implemented these exchanges for each interChange state and has addressed the current HIPAA requirements. The interfaces for the formal healthcare transaction sets will be performed through our interChange Connections Electronic Data Interchange (EDI) solution.

Additionally, HP will work with the Department to determine what proprietary file formats and Colorado-specific interfaces will need accommodation and recommend the most appropriate transfer method. The Colorado interChange MMIS solution will provide comprehensive interface capabilities required to support the stakeholders who have direct data interaction with the MMIS.

When designing our strategy and approach to receiving, processing, verification, notification, reporting, monitoring, administration, and security related to the Colorado interChange MMIS, we use our experience to assemble the best practice features for the stakeholders. Our strategy is straightforward and is based on the philosophy of transferring proven data receipt and processing capabilities to the Department.



Based on our experiences, we realize that the many stakeholders that deal with the MMIS are at various levels of technology sophistication. Our proposed solution takes a common-sense approach of providing the right technology for the right business value at the right time. This approach has been proven successful in real life through multiple MMIS implementations and subsequent operational support.

The details of the approach include using our interChange Connections capabilities, using secure FTP (SFTP) and the interChange MMIS service-oriented architecture (SOA) as a key interChange MMIS interface solution. We understand that not every entity is ready for SOA integration; our solution has a suite of interfaces that meets the various needs of stakeholders in many states. The integrated architecture made possible through SOA is responsive, resilient, and reliable. The Department gains better visibility into enterprise information and quickly adapts applications to changing business processes. The reusable assets, standard processes, and extensive national and global experience brought by HP's approach to SOA will deliver the improved accessibility and flexibility. The SOA design also reduces operational maintenance costs by simplifying the process of making changes by having a single service applicable to multiple business processes. For example, a single service can facilitate a response from the automated voice response system (AVRS) while enabling the same type of responses through the

self-service provider web portal. Using the proposed Colorado interChange MMIS architecture, HP can respond faster to regulatory, programmatic, and technology changes because the SOA is adaptable and extensible.



The Colorado interChange MMIS will have an Enterprise Service Bus (ESB) that allows for inbound and outbound interface management. interChange Connections provides EDI and ESB capabilities. The SOA ESB supports services such as content management, AVRS, and web portal interfaces. ESB is an architectural construct and is a core feature of middleware technology. It provides a layer of abstraction on top of the integration and messaging backbone. The ESB provides the capability to expose business application functions as reusable assets within an offering.

The interChange Connections module supports EDI processing for claims, eligibility, prior authorization (PA), point of service (POS), providers, and managed care organizations (MCOs). Connections also supports the other interfaces needed to operate the MMIS transactional processing system.

HP interChange Services



interChange Connections, the HIPAA-compliant system, is based on a three-tier architecture that separates external (Internet) communication, application, and data layers. Reliability and performance are the foundation of interChange's clustered infrastructure that is built to deliver high-availability, fault-tolerant, and highly secured EDI services. The architecture is flexible, scalable, and allows for rapid document turnaround. It can quickly integrate, manage, and automate dynamic business processes by exchanging business documents among applications, within or across organizational boundaries. The interChange solution is extensible, so that additional services can be transparently integrated.

interChange uses Edifecs commercial off-the-shelf (COTS) software for the data file format validation. interChange has successfully employed this method of data verification and quality reporting of the inbound file structures. The Edifecs XEngine Server is one of the most widely used run-time engines for validating and converting legacy file formats, such as EDI, HL7, HIPAA, and flat files, to and from XML.

Features of the interChange MMIS EDI solution include the following:

- Single interface to providers and clearinghouses
- Batch and interactive routing
- HIPAA compliance service:
 - Certified quarterly for edit types 1-7 for ASC X12N transaction and code sets
 - Claim-level and document-level rejections
 - Uniform submission response reports

- Ability to set edits to a warning status
- Code set validation can be set by transaction type or version
- Monthly code set updates
- Privacy and security compliance
- Duplicate claim checking
- Data mapping and translation—any-to-any, one-to-many, and many-to-many: ASC X12, XML, and proprietary formats
- Help desk support 24 x 7
- Support for multiple environments
- Capacity planning
- Performance analysis and system tuning
- Redundant network
- Message routing, security, and tracking
- Transaction audit tracking reports

While the interChange Connections is the primary means of data receipt, validation, and processing, the overall MMIS provides many diverse data receipt access channels. The following is a summary of those channels:

- Connections for EDI
- AVR
- Direct submission (SFTP)

interChange uses various features and components of these systems while verifying file integrity. The following hardware and software components comprise the interChange solution:

- The web tier comprises multiple, load-balanced servers.
- The application tier is running clustered servers across redundant servers for high availability and load balancing.
- The web and application tiers run Windows Server 2008R2 and each of these tiers are scaled and provisioned with VMware vSphere. This provides the virtualization layer that maximizes the computing infrastructure that is powered by HP ProLiant Blade Servers.
- The database tier is running Oracle 11g Database Servers with Real Application Clustering (RAC) for high availability. This environment is fortified with a failover environment required to meet the Department's uptime requirements.
- HP TippingPoint Network Intrusion Detection appliances and firewalls secure the network.

- Edifecs XEngine Server COTS software parses files and HIPAA validation and performs edits, generates acknowledgements, and reports.
- BizTalk Server—ESB engine. The translation engine has the capability to code specific and unique business rules and to verify that these rules are applied when certain conditions are satisfied. Additionally, BizTalk Server is used for workflow management and business activity monitoring

HP Healthcare Portal

The HP Healthcare Portal is compliant with HIPAA security regulations to safeguard member privacy. The portal adheres to National Provider Identifier (NPI) standards for HIPAA-standard transactions and is content-compliant for inbound and outbound transaction sets, such as the ASC X12 276/277 and 837 I, D, and P. The adoption of the web portal for real-time claim adjudication is a provider-friendly component of the overall Colorado interChange MMIS as the provider community realizes the value of direct data entry for claims and seeing the adjudication resolution for the claims immediately.

The Colorado interChange data receipt and data delivery management solution is built on a proven set of capabilities. The selected options for Colorado interChange MMIS data receipt and data delivery management are solutions already running in production environments and have solved the real-world challenges proving the ability to integrate into a healthcare delivery environment. This built-in operational knowledge and experience has demonstrated the flexibility, scalability, extensibility, and the long-term supportability and maintainability of our interChange Connections module.

Additional Solution Details

Besides the technical solution, the data receipt solution will have dedicated resources to support and maintain the solution. The Colorado interChange MMIS and portal are supported by a product help desk. The interChange Connections accepts HIPAA transactions and represents the logical production architecture that will be deployed for this implementation.

Channel management is responsible for the physical connectivity and communication protocols between trading partners and the interChange MMIS. Channel management comprises physical connectivity, communication protocols, and the business processes used to support the exchange of healthcare-related traffic in compliance with HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH) privacy and security regulations.

Physical trading partner connectivity comprises the following:

- Internet
- Direct connects
- HP EIN (HP internal network)

Supported communication protocols include the following:

- Queuing (MQ, AQ, JMS)
- HTTP, HTTPS
- Web Services/SOAP
- VPN
- SSH, SSL
- SFTP, FTPS
- Connect: Direct (NDM)
- TCP/IP sockets
- AS2
- FTP PGP

Batch Control, Balancing, and Scheduling of Data Load Cycles (Unique ID 1154)

HP will coordinate data exchanges with other contractors and Colorado agencies. After a data exchange window has been decided, the actual exchange can be fully automated using configurable tools such as AutoSys for batch control and interChange Connections File Transfer Services (interChange FTS).



The FTS component in interChange Connections monitors, tracks, logs, and moves files throughout the interChange solution. The FTS portal interface provides full audit tracking of files and notifies users of errors that occur during file transfers. Key features of FTS include the following:

- Archives transferred files
- Renames files
- Checks for duplicate files
- Compresses and decompresses files
- Transfers file using file copy (UNC) FTP, FTPS (SSL technology), and SFTP (SSH technology)

Infrastructure Hardware and Software Updates (Unique ID 1157)


HP implements numerous enterprise tools that enable us to fully manage the purchase and maintenance of infrastructure hardware and software. This encompasses updates, firmware, upgrades, and technology refresh targets to maintain the of the interfaces.

HP will provide a detailed management schedule during the Implementation Phase. HP uses ITIL v3 reference architecture practices to include the following:

- Ticketing and workflow
- Incident, problem, and change management
- Configuration management
- Asset and license management


- Event management
- Availability and capacity management
- Service-level management
- Request management

After agreement of the scope and terms of the contract, HP will complete an architecture design document that will include descriptive lists for the infrastructure applications, hardware and software infrastructure bill-of-materials. The architecture design document will be reviewed and approved by the Department to verify agreement for the overall solution. HP has internal procurement processes allowing for tracking from order to delivery.

 HP will deliver the approved technical infrastructure and computing environments within the HP data center. Each hardware and software item will have detailed installation and configuration procedures described in the engineering guide. During implementation, each asset will be included within the HP inventory and CMDB. Software and hardware that are installed after the initial project setup will follow the change control, detailed installation, and qualification processes. HP has detailed work instructions, with associated quality assurance verifications, to validate that our architecture design document and engineering guides are maintained.

HP uses inventory, package distribution, and asset and audit compliance tools for continual management allowing consistent deployments, increased automation, and recurring updates.

Asset Management

 HP maintains an IT asset repository of the technical infrastructure assets. The HP IT Asset Management system provides greater financial control, with significant costs savings, by tracking and reporting on data elements relating to ownership, status, age, and location of IT hardware and software assets. HP manages these assets throughout the IT asset life cycle in full compliance with industry regulations. Managed assets include computers, contracts, licenses, warranties, and maintenance service agreements. Additionally, HP will enable universal auto-discovery that provides accurate and prompt updates to the repository.

Our proven asset management process will accomplish the following:

- Verifies HP IT hardware and software assets are registered, represented once, and maintained in the IT asset repository
- Reduces or eliminates unnecessary costs, such as lease and rental penalties for missed deadlines of third-party assets
- Reduces software license expenses by tracking compliance and determining when additional software licensing is required
- Identifies when upgrades and patches are available to individual infrastructure resources

- Schedule the proper release of updates, upgrades and refresh activities to minimize impact to the system
- Captures IT asset information for installations, moves, adds, changes and de-install (IMACD) activities, including support details (such as maintenance contracts)
- Proactively identifies IT assets to be refreshed or retired and tracks the time line for these actions to occur

The asset management process includes the following eight subprocesses:

- Creating, or modifying, the IT asset management plan—Our IT asset new business analyst accomplishes the following:
 - Determines the scope of the IT asset management services being requested
 - Identifies the scope of the IT hardware assets and software licenses that require tracking
 - Identifies the technology and solution requirements, including discovery tools and IT asset repository
 - Identifies customer-specific requirements that prevent the implementation of a standard asset management solution
 - Determines the program staffing and resource requirements
 - Verifies the technical solution enables the successful delivery of IT asset management services
- Receiving the IT assets—Our IT asset receiver accomplishes the following:
 - Performs a verification of the supplier's shipping documentation, validates items received, and identifies discrepancies between the items ordered and the items received
 - Stores IT assets before placement in the customer's environment
 - Validates the supplier's affixed IT asset tags
 - Assigns and affixes IT asset tags
- Maintaining and controlling the IT assets—Our IT asset manager accomplishes the following:
 - Receives and validates IT hardware and software assets with contract information
 - Gathers IT asset data required for the registration of hardware and software license assets, including the associated contract records such as lease, warranty, and hardware maintenance agreements
 - Documents and addresses hardware asset record discrepancies
 - Identifies, documents, addresses, and resolves hardware asset data attribute discrepancies

- Performs bulk loads of IT software asset data to support steady-state IT asset management
- Verifying and auditing the IT assets—Our IT asset manager accomplishes the following:
 - Analyzes IT asset information requirements and determines the correct method of providing information to the requestor; achieved by performing a physical audit, spot audit, or providing reports
 - Determines if verification requirements can be addressed with standard reports, and whether ad hoc reports are required
 - Follows verification and auditing activities, and identifies IT asset discrepancies, including required updates to the IT asset repository
 - Provides audit and verification results, including reports, to the requester or the Department
 - Reviews software inventory and license compliance reports with the Department to provide recommendations to resolve instances of noncompliance
 - Initiates problem records to investigate the source of major data discrepancies between the IT asset repository and the production environment
- Updating the IT asset repository—Our IT asset manager accomplishes the following:
 - Creates and modifies the hardware asset records in the asset repository
 - Creates and modifies contract records in the IT asset manager relating to hardware assets, such as lease schedules and maintenance agreements
 - Performs bulk loads and updates of hardware asset data to support steady-state asset management
 - Requests enhancements to the master data repositories
 - Monitors automatic loads of asset information from external sources and addresses identified discrepancies or errors
- Maintaining the software license compliance—Our IT software license compliance administrator accomplishes the following:
 - Reviews new in-scope software publisher and title information received during operations
 - Creates software title counters in alignment with contracted software license compliance tracking service requirements
 - Determines customer's license position through the execution of software title counters
 - Modifies and deactivates software title counters to promote accurate reporting

- Maintaining Software Application Index (SAI) libraries—Our IT software library administrator accomplishes the following:
 - Analyzes and investigates executable files that are not recognized by the HP Discovery and Dependency Mapping Inventory (DDMi) scanning tool
 - Teaches applications associated with unrecognized files by the HP DDMi tool to the HP User SAI Library to enable future recognition by DDMi
 - Reviews new in-scope software publisher and title information received during on-boarding and steady-state operations to determine the effect on the HP/HPSS SAI libraries and the product registry
 - Submits requests to add software models to the product registry
 - Identifies new software applications for the HPSS Master SAI Library
- Releasing SAI libraries—Our IT software library administrator accomplishes the following:
 - Reviews modifications to the HPSS Master SAI Library and identifies requirements to add software installation models to the Product Registry
 - Packages new applications into the HP SAI Library for release into the client’s environment
 - Documents release notes about new HPSS and HP SAI libraries
 - Formally releases updated HP and HPSS SAI libraries into the production environment

Asset Management Process Overview

Our asset management process will cost-effectively manage assets through their entire life cycle, from installation to deposition, in full compliance with regulatory requirements. The following figure provides a high-level asset management process flow, the interrelationships of the subprocesses, and the key personnel.

The following figure details the color-coding scheme that matches the HP Asset Management personnel—listed on the left-hand side—to the activities they manage within the process.

Software Development Life Cycle

HP uses an EDGE SDLC methodology to lead and support enterprise projects, including custom software builds, COTS implementations, and the transfer of existing systems such as enhancements. This SDLC is repeatable, refined from decades of hands-on experience and industry best practices from organizations, including the following:

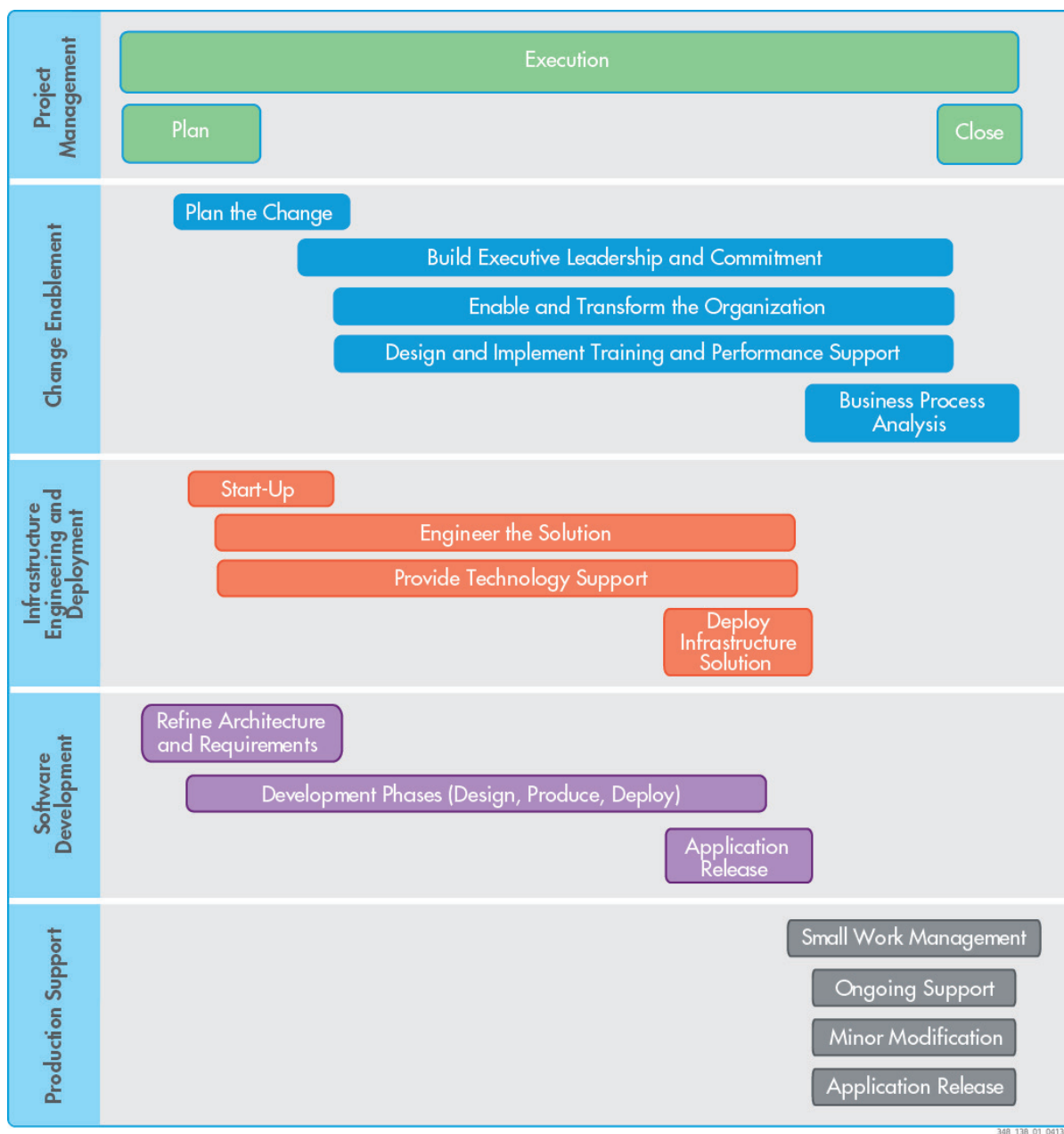
- Institute of Electrical and Electronics Engineers (IEEE) 12207-2008 – System and Software Engineering—Software Life Cycle Processes
- IEEE 1058-1998, Standard for Software Project Management Plans
- Project Management Institute’s (PMI’s) *Project Management Body of Knowledge* (PMBOK)
- Alignment to Capability Maturity Model Integration (CMMISM) Level 4 and International Organization for Standardization and International Electro-technical Commission (ISO/IEC) 12207:2008

The best methodologies are not a static set of didactic tasks that need to be checked off during a project. The HP SDLC serves as an overarching guideline designed to integrate with our project management processes, along with those of the customer’s project team.

As illustrated in the following figure, the Project Management component of the SDLC ties our PMI PMBOK processes to the SDLC, from planning through turnover. The Infrastructure Engineering and Deployment component of the SDLC comprises the activities that will be used to perform infrastructure architecture development, solution design, maintenance, and deployment. The Software Development component comprises three major processes of the Development Phase: application design, production, and deployment. This is followed by an application release that incorporates testing, installation, training, and start-up support.

The SDLC provides a proven and flexible set of processes, procedures, standards, tools, templates, and training to support the delivery of a premium, efficient solution as illustrated in the following figure.

The HP SDLC



Fiscal Agent Operational Data (Unique IDs 1164, 1166)

Fiscal operational and systems data required for reporting and analysis will be provided to the BIDM. HP will work with Department's staff during implementation to verify the necessary data and format is delivered to BIDM promptly using interChange Connections.

Through the enterprise service bus capabilities supplied as part of Connections information and data management with reliable and measured delivery is performed. Through the Connections FTS windows managers can check on the status of data transfers to BIDM to make sure the data was delivered.

Audit Trail (Unique ID 1215)

The FTS component of interChange Connections monitors, tracks, logs, and moves files throughout the Colorado interChange solution. The FTS portal interface provides full audit tracking of files and notifies users of errors that occur during processing as shown in the following figure. Additionally, data fields in the HP MMIS maintain an audit trail.

**RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED**

The Search screen lets the user find a file quickly and easily, determining at a glance the status, processing phase, and file details. This provides a complete picture of the transaction as it progresses through the Colorado interChange MMIS. Having the ability to research the status of MMIS inputs and outputs is a significant improvement and advantage of the interChange Connections offering. Research previously limited to technical resource is now smooth and available to the operations staff.

We further describe MMIS audit details in RESPONSE 38m.

Interoperability (Unique IDs 1248, 1249)

Interoperability of the new MMIS is powered by our interChange Connections component that orchestrates interaction of the MMIS with the broader healthcare ecosystem. interChange Connections is driven by the BizTalk Server, which can be used for interfacing with statewide HIE, EHR, PHR, and HIX. The following figure illustrates the role played by interChange Connections as the gateway between the MMIS and the related healthcare entities.

(1249) A fundamental purpose of the BizTalk server is to support the integration of the MMIS with external applications while enabling the communication between the MMIS and those applications through defined services. The important part of meeting this requirement is that the core framework and integrated tool solution based on BizTalk positions the Department for expanding interoperability between the MMIS and other entities throughout the life of the contract such as the expansion to include HIE, HIX, BIDM, and COFRS components.

(1248) As part of the interChange MMIS implementation, HP will work with Department staff members to create data exchanges. The following are examples of existing data exchanges:

- Real-time claim adjudication for claims—Providers and clients can interact with the MMIS using the Internet through the HP Healthcare Portal, which supports the distribution of program information, the submission of claims and client eligibility validation, and other features.
- The web-based prior authorization (PA) application process enables providers to submit authorization requests including the uploading of appropriate attachments through the web portal.
- Web-based distribution of the RAs is available.
- Web-based access to claims for claims corrections, resubmitted, adjustments or roster billing. Providers or their designated representative can search by multiple claim data elements.
- Automated services are compliant with ACA1104 Core Operating rules for exchange of covered transactions.

HP will work with Department staff members to build services and tools that will meet the present and future needs of the Colorado interChange.

Detailed Connectivity Guides (Unique ID 1250)

For external users, HP will maintain and publish a detailed connectivity guide that contains the data dictionary to define external contracts and service connection protocols through the web portal. HP will maintain a system object model, accessible to appropriate Colorado and internal staff members that will detail the relationship between business objects and the database data model.

For internal users, access to a common, integrated, fully attributed data dictionary will be provided through the Help feature in the interChange MMIS. Authorized users will select the Help feature from the menu bar, and then select Data Element Dictionary from the available options as illustrated in the following figure. The data dictionary fields will contain: plain English field names, field descriptions, database field name, database table, field type and length, associated codes, code descriptions, and original source.

RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED

System Interfaces and Integrations (Unique IDs 1256, 1262)

The VITAL platform can interface with case management systems and link that data to client and client claims/encounter records. The platform uses ASCII based flat files and supports the use of common web formats, such as X12, XML, and other proprietary formats. The format and messaging method depends on the Department's implementation needs. HP and the Department will determine the appropriate interface between interChange and the platform to verify the proper alerts are triggered within the application. For example, the Department can refresh data in about new conditions and risk scores, then assign to a user's work list for follow-up.

Financials (Unique ID 1258)

HP will support the financial process by developing a customer interface developed during DDI to send appropriate accounting information through COFRS for each program integrity and Department's recovery, offset, or adjustment. The customer interface will produce reports to validate that everything remains balanced and accurate.

Relevant Federal and State Databases (Unique IDs 1465, 1466)



A data service from LexisNexis will be used to meet the requirements of Rule 6028 of the Affordable Care Act (ACA) for provider credentialing and background checks. (1465) LexisNexis pulls information from a large database of public and proprietary records to give a detailed view of

individuals or businesses and their history. This service aids in the investigation process by quickly identifying fraud and other incidents within the last five years that involve the owners, indirect owners, and managing employees.

LexisNexis compiles reports on companies and individuals associated with a tax ID or Social Security number. These reports can include such information as civil judgments and liens, bankruptcies, court and regulatory rulings, negative news, and felony charges. LexisNexis also can validate and authenticate the identification credentials of potential providers.

Automatic interfaces to LexisNexis contain provider information and the names of individuals and entities listed on the disclosure forms, including managing employees and individuals with more than a State-defined percentage interest in the business. We will work with the Department to define processes for providers with negative information identified during screening and determine the frequency of file submissions to LexisNexis.

We understand the importance of screening applications according to Department rules. These rules are in place so only legitimate providers are allowed to participate in Medicaid. The Department can screen provider data including the following:

- State and federal sanctions
- NPI validation
- License or certification validation
- Specialty board certification
- Civil and criminal background checks
- Deceased status
- Medicare verification
- Address verification
- Tax number information—IRS TIN or Social Security number

The provider enrollment framework uses rule-based workflow to verify enrollments. This flexibility allows the Department to easily change workflow such as adding new requirements such as on-site visits or additional interfaces. During DDI, we will work with the Department to define these workflows so they align to State and federal guidelines and also clearly define the roles that HP and the Department play in the workflow cycle.

(1466) During the DDI the HP team will work with the Department to identify the specifics around the upload sanctioned, terminated, exclusions and other required information to federal databases, in accordance with ACA Provider Screening Rule. In support of federal legislation the HP healthcare team has a dedicated set of individuals who interpret legislation and then share the information with our many accounts.

Pharmacy Claims from the PBMS (Unique ID 1517)

HP understands the importance of uniquely identifying transactions or claims—such as ICN for claims. Just as the PBM uniquely identifies their claims, HP assigns a unique ICN to each

pharmacy claim received from the PBM for tracking and control purposes. HP maintains the unique identifier assigned by the PBM and cross-references this identifier to the HP-assigned ICN. It is important to maintain the PBM's unique identifier for the following:

- Correspondence or communication with the PBM
- Identifying which claim the PBM is reversing
- Identifying the original claim in an adjustment situation
- Research of pharmacy claims in the MMIS

HP claims inquiry allows claim lookup by the PBM's claim identifier. This greatly aids research for users who work with the PBM and may only know the PBM's claim identifier. HP has experience loading pharmacy claims from subcontracted PBM vendors and state-contracted PBM vendors on various schedules:

- Florida HP runs daily more than 100,000 pharmacy claims
- Georgia HP runs weekly more than 250,000 pharmacy claims

This experience of working with external PBM vendors gives our team strong insight into the critical nature of clear communication, testing and validation in the area of pharmacy processing. The lessons learned from these experiences will be applied to the COMMIT project.

Claims and Encounter Payment Information Reconciliation (Unique ID 1520)

Financial Processing Overview

The Financial Processing function encompasses claims payment processing, accounts receivable, and nonclaim-related expenditure processing. It verifies that the funds are appropriately disbursed for claim payments and recovery transactions are accounted for and applied accurately. Among the processes that the Financial Processing function includes are the generation of payments to payees and the production of an 835 remittance advice for each payee or one available to providers through the web portal. The payments can be made using paper check or an electronic funds transfer (EFT). The provider maintains extensive information and features such as establishing and modifying their payment method through the Provider Self-Service function on the web portal.

Payment Voids

Several types of payment voids can be performed in the Colorado interChange:

- Paper check payment voids include the following:
 - Void—Executed when payment is rejected by payee, and the fiscal agent physically has possession of the check
 - Stop pay—Executed when payment is rejected by the payee, and the fiscal agent does not have possession of the check

- Reissue—Executed when a stop payment was requested as a replacement by the payee because of a payment not received
- EFT voids include the following:
 - Reversal—Executed within five days of the payment date to create an EFT debit transaction to settle concurrent with the EFT payment, negating the original payment sent to the State’s bank
 - EFT fail—Executed after receiving notification from the state’s bank that an EFT payment sent was rejected for reasons indicated on the failed electronic notification back to interChange from the bank, such as account closed

Reconciliation

Reconciliation in interChange includes the following:

- **Staledating**—If the Department defines a length of time they want a warrant to remain outstanding but then to be staledated, it means to return the funds to their original source after this defined length of time as though the expense did not occur. If the warrant is later offered for payment and the Department policy is to allow the payment, the interChange system will request the monies as a new expenditure but use the Federal Medical Assistance Percentage (FMAP) of the original expenditure to correctly fund the warrant.
- **Bank issues and clears processing**—Following each financial cycle, an issues file is sent to the State’s bank with EFT and paper check information. As these warrants clear, are voided, reissued, or staledated, updates are sent from interChange to the State’s bank. Monthly, the State’s bank sends interChange a clears file to update the statuses of the warrants and EFTs based on their account activity. The Colorado interChange provides the capability to hold payment transactions based on the Department’s user-defined criteria. The hold process takes place during a scheduled payment cycle configured to execute the payment hold process. Held transactions are delayed from finalizing until the next payment cycle or a subsequent payment cycle as defined by the Department user. Payment hold transactions are recorded and can be queried online using the Payment Hold Transaction panel in interChange.

We detail the capability of HP’s MMIS Financial System including payments, recoupment and adjustments in RESPONSE 39c.

Claims Payment Tracking Details (Unique IDs 1600, 1626)

Payment Review and Release

The interChange financial system processes payments on various schedules for the different defined payers in a multi-payer system. When the cycle completes, several reports are generated to allow the Department to review the activity and payments generated before approving the cycle for release. Each payer’s department has set procedures for how to review the received reports to approve that cycle’s check-write. When approved, an authorized Department user

accesses the Financial Related Data Payment Release panel to approve and authorize that financial cycle. This release triggers the interChange system to release the payment bank files to the print center, if applicable, and the State's bank for processing of the EFTs. (1600) The EFT, warrant number is permanently stored as part of the claim history.

Scheduling

The Colorado interChange scheduling process has four functions:

- Determine payers and payees to process in a financial cycle, and establish the frequency and special functions allowed in that financial cycle's schedule
- Determine the specific claim type or status and financial transactions to allow in the financial cycle
- Determine special processes allowed on that schedule, such as payment deductions.
- Associate reports to be generated out of the scheduled financial cycle

(1626) As part of the overall solution, the interChange MMIS has the interoperability to receive information from BIDM which can be used when configuring edits or suspense of payments before check write and the rationale for the claim going into suspense status. The functional capability within the interChange MMIS that enables holding payments for providers is referred to as 'fiscal pend' and prevents payments from occurring while a provider is on fiscal pend.

Client ID Discrepancies (Unique ID 1649)

HP provides weekly and monthly operational reports of the link and unlink requests processed. Operations staff members can request that clients be linked or unlinked through the UI panels. Through operational procedures, staff members verify if the client is the same person under two different IDs. After the verification is complete, they request the link or unlink and it is identified on the reports with specific data that was not linked or unlinked.

Additionally, an automated process creates a pseudo ID for new clients. The Colorado interChange calls the MCI system, which correlates the client with the pseudo ID. The client is automatically linked and appears on the report.

BIDM Reports (Unique IDs 1707-1709)

(1707) The required case management data is available. HP will supply the required information to BIDM in order for that vendor and application to support the coordination of care for clients.

(1708) Survey capabilities will be provided through the tool Survey Monkey which provides an easy to use and cost-effective survey feature. (1709) The ability to collect, track and search health demographics information is provided through McKesson's case management for effective organization and management of this key data for assistance and analysis of client healthcare data. We detail this requirement in RESPONSE 39g.

Preexisting Provider-Client Relationships (Unique ID 1718)

Colorado interChange provides the ability to assign a client to a previously-assigned provider, given the provider is available and is still appropriate for the client's eligibility category.

EDMS (Unique ID 1723)

Because the Colorado interChange is based on a business service framework, many of the associated EDMS tasks such as attaching supporting documents, creating and tracking correspondence, and analyzing detailed business process metrics to drive efficiencies flow together naturally in a universal, next-generation approach. Additionally access to EDMS content is carefully controlled using role-based security to establish compliance with HIPAA privacy and security requirements regarding security of protected health information (PHI).



The following figure depicts a workflow instance that manages the process of taking a scanned document and uploading it into the EDMS. Imaging a document is a triggering event that will invoke a web services request and send inputs such as extracted client contact information to the interChange Business Services.

RESPONSE HAS BEEN GRANTED CONFIDENTIAL TREATMENT BY THE
DEPARTMENT AND HAS BEEN REDACTED

The interChange Business Services Workflow engine starts a workflow for uploading an imaged document. The workflow instance can generate and assign work items to humans or service-enabled applications.



Workflow will upload documents to the EDMS through a web service call. The same connectivity and interaction is available to service-enabled applications, such as the correspondence generator or the contact tracking management system. This workflow capability extends document management far beyond the user interface and into a network of configured applications and processes.

We provide additional detail about the Colorado EDMS solution in RESPONSE 39j.

Long-Term Level of Care Determination Processes (Unique ID 1744)

The VITAL Platform can flag clients for long-term level of care. New and modified authorizations are part of the extract files sent to Colorado interChange. These flagged records are then passed back to the source eligibility systems, including CBMS and TRAILS.

Case Management Tool (Unique ID 1754)

HP will work with the Department to develop the integration that allows case managers to access information from and input information to EDMS using the single sign-on (SSO) solution. Provider correspondence, case management correspondence, and other external information are refreshed into the VITAL Platform through a nightly batch refresh process. This information also can be attached to the client's record through the Notes function.

Support Intensity Scale Data (Unique ID 1761)

The care management VITAL Platform will support the ability to accept Support Intensity Scale (SIS) data from the SIS Online system. HP will work with the Department to determine the information for uploading and frequency of the upload.

Pharmacy Content Access (Unique ID 1774)

As part of the Healthcare Portal, we will configure the solution to include the following:

- Web announcements
- Training schedules and enrollment
- Information on the diabetic supply program
- Various forms including prior authorization form
- Information on maximum allowable costs
- Information on preferred drug lists
- Information on prescriber lists
- Pharmacy meetings

We will coordinate with the selected PBM vendor and the state to gather the content and publish the most recent versions of this information on the portal for the provider community.

We detail the portal in RESPONSE 391.

TPL Carrier Files (Unique ID 1846)

The Colorado interChange stores TPL carrier and resource information including historical data. Carrier data is maintained by updates through the online panels. The Colorado interChange also supports the ability to perform mass updates through the online panels.

TPL resource information is updated through the panels and through interface files between the Colorado interChange, insurance carriers, TPL vendors, and others. Clients and providers also can update TPL information using the web portal—subject to HIPAA requirements.

Data Exchanges with Insurance Carriers and Governmental Agencies (Unique ID 1848)

HP will provide data to the Department's contractors and government agencies interfaces. We will define the contractor data exchange interface during the DDI Phase. As previously described interoperability between the MMIS and other stakeholders is securely managed through the interChange Connections module.



HP will recommend and perform data exchanges with the Department's contractors, insurance carriers, governmental agencies, and other entities as authorized and directed by the Department. HP understands that maximizing TPL collections requires a series of electronic exchanges that use specially selected multiple match keys performed on the widest network of carrier files.

Each successful data exchange provides the Department an opportunity to reduce overall expenditures by verifying Medicaid is the payer of last resort. For many of our other states, HP performs the data matching activities. By performing cross matches with eligibility files from health insurance, commercial carriers, and other governmental agencies, HP can identify and verify previously unknown third-party coverage information for Colorado's Medicaid clients.

Medicare Participation Information (Unique ID 1849)

The Colorado interChange complies with the requirement to accept Medicare participation files. HP will maintain and update Medicare participation information when received from external sources. Automatic updates of Medicare information will be received from CMS. This Medicare data will update the Colorado interChange. The HP Operations team also can update Medicare information using the Colorado interChange panels.

Premium Payment Billings from CMS (Unique ID 1853)

The Medicare Buy-In Program allows states to pay Medicare premiums for dually eligible (Medicare and Medicaid) clients, thereby facilitating Medicare enrollment. Because Medicare is usually the primary payer, payment of the Medicare premiums, coinsurance, and deductibles is more cost-effective than paying the entire cost of a client's medical care. The State receives federal financial participation (FFP) for premiums paid for clients eligible as qualified Medicare

beneficiaries (QMBs), qualified disabled working individuals (QDWIs), specified low-income Medicare beneficiaries (SLMBs), Money Grant clients, and qualified individuals (QI-1s).

The primary goal of the Prepare and Pay Premium Payment process is to optimize cost avoidance by making appropriate buy-in payments for eligible clients.

Overview of Vendor Buy-in Solution

The Colorado interChange Buy-In system complies with State and federal policy and regulations and uses a combination of daily and monthly processes to enroll those with dual eligibility as quickly as possible. Several processes comprise the Buy-In cycle. The receiving process accepts the incoming billing/response records from CMS. Eligibility validation decides the accretions and planned deletion records based on current client data. Accretions and planned deletions are stored in the buy-in tables waiting for the subsequent process. The sending process concludes the buy-in cycle and creates the buy-in premium request records—such as accretions, deletions, and changes—that the Colorado interChange sends to CMS.

Throughout the month, the Department and HP buy-in analysts will complete manual activities to resolve mismatches and exception responses from CMS. The HP buy-in analyst applies updates on the user-friendly buy-in user panels.

Each of the primary buy-in processes updates the Colorado interChange client tables and creates activity and audit trail reports. The Colorado interChange Buy-In system provides data exchanges, reports, and panels that support various functions including the following:

- Sending and receiving Medicare Part A, Part B, and Part D billing and response file
- Validating eligibility, co-insurance, and deductible payments
- Processing and maintaining data
- Resolving data exchange issues
- Initiating manual adjustments to resolve problems preventing client buy-in
- Reconciling transaction errors
- Paying premiums and obtaining refunds

Business Process Description

The Prepare and Pay Premium Payment business and automated processes comprise exchanging data, verifying coverage, resolving issues and mismatches, paying and refunding premiums, reporting data, and recruiting Medicare B clients.

Exchanging Data



Timely and accurate data exchanges are critical to the buy-in process. The Colorado interChange uses daily processing of files from ICES, SSA, and CMS. Particularly, daily processing of the CMS Territory Based Query (TBQ) system data that allows states to retrieve the Medicare Master Beneficiary Data and daily BENDEX data enable HP to enroll clients in buy-

in within days rather than months. The same MMA file layout used by Part D enrollment exchanges the TBQ data. In other states, HP is replacing the EDB process with TBQ because of the wealth of data provided. We propose this same approach for the Department. CMS strongly encourages states to use TBQ. This can significantly increase a state's cost-avoidance.

Validating Eligibility and Coverage

Several resources are available for identifying potential Medicare buy-in clients. During the receiving batch process, the system attempts to locate and match CMS client record to the Colorado interChange client record with two criterions:

- If the Colorado interChange locates and matches the client, the CMS record is a “match.” CMS match records update specific Colorado interChange tables and users view them on UI panels. The Medicare Buy-In Part A records update tables and display on panels specific to Part A. The Part B records update tables and display on panels specific to Part B.
- If the Colorado interChange does not locate and match the client, it processes the CMS record as a “mismatch.” CMS mismatch records update specific tables and display on user panels. During the validating process, HP analysts identify clients to “accrete” (add) and delete. The Colorado interChange fully supports client accretion and deletion.

The buy-in process updates client Medicare data for Part A, Part B, and Part D when received from CMS and SSA. The daily exchange of data providers tighter controls on inappropriate payments. The buy-in analysts monitor reports for Medicare client date of death to prevent payment of buy-in premiums for periods after the date of death. However, this step is a formality because if CMS shows a date of death on file, it will not accept a premium payment billing transaction.

If CMS updates a date of death retroactively to its file and the State has paid premiums after the fact, CMS refunds inappropriately made premiums with a code 16 transaction. If the Colorado interChange shows a date of death on file and CMS is billing for premiums, the Colorado interChange generates a code 53 transaction to stop buy-in.

Resolving Issues and Mismatches

Medicare client-related information is stored in the system. The system maintains audit tables and log files of files received through the various data exchanges. The client information is available in user-friendly panels and reports. The online information and reports facilitate quick issue resolution for buy-in-related issues including resolving mismatches and buy-in errors.

We detail payment billing and buy-in procedures in RESPONSE 40g.