SOLICITATION #:

2017000265

Appendix JJ

HIPAA BAA

HIPAA BUSINESS ASSOCIATE ADDENDUM

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

RECITALS

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

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

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

The parties agree as follows:

1. Definitions.

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

b. "Protected Health Information" or "PHI" means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be

used to identify the individual, and shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.501.

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

d. "Subcontractor" shall mean a third party to whom Associate delegates a function, activity, or service that involves CE's Protected Information, in order to carry out the responsibilities of this Agreement.

2. Obligations of Associate.

a. Permitted Uses. Associate shall not use Protected Information except for the purpose of performing Associate's obligations under this Contract and as permitted under this Addendum. Further, Associate shall not use Protected Information in any manner that would constitute a violation of the HIPAA Rules if so used by CE, except that Associate may use Protected Information: (i) for the proper management and administration of Associate; (ii) to carry out the legal responsibilities of Associate; or (iii) for Data Aggregation purposes for the Health Care Operations of CE. Additional provisions, if any, governing permitted uses of Protected Information are set forth in Attachment A to this Addendum. Associate agrees to defend and indemnify the Department against third party claims arising from Associate's breach of this Addendum.

b. Permitted Disclosures. Associate shall not disclose Protected Information in any manner that would constitute a violation of the HIPAA Rules if disclosed by CE, except that Associate may disclose Protected Information: (i) in a manner permitted pursuant to this Contract; (ii) for the proper management and administration of Associate; (iii) as required by law; (iv) for Data Aggregation purposes for the Health Care Operations of CE; or (v) to report violations of law to appropriate federal or state authorities, consistent with 45 C.F.R. Section 164.502(j)(1). To the extent that Associate discloses Protected Information to a third party Subcontractor, Associate must obtain, prior to making any such disclosure: (i) reasonable assurances through execution of a written agreement with such third party that such Protected Information will be held confidential as provided pursuant to this Addendum and only disclosed as required by law or for the purposes for which it was disclosed to such third party; and that such third party will notify Associate within five (5) business days of any breaches of confidentiality of the Protected Information, to the extent it has obtained knowledge of such breach. Additional provisions, if any, governing permitted disclosures of Protected Information are set forth in Attachment A.

c. Appropriate Safeguards. Associate shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by this Contract. Associate shall comply with the requirements of the HIPAA Security Rule, at 45

C.F.R. Sections 164.308, 164.310, 164.312, and 164.316. Associate shall maintain a comprehensive written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Associate's operations and the nature and scope of its activities. Associate shall review, modify, and update documentation of its safeguards as needed to ensure continued provision of reasonable and appropriate protection of Protected Information.

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

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

f. Access to Protected Information. If Associate maintains Protected Information contained within CE's Designated Record Set, Associate shall make Protected Information maintained by Associate or its agents or Subcontractors in such Designated Record Sets available to CE for inspection and copying within ten (10) business days of a request by CE to enable CE to fulfill its obligations to permit individual access to PHI under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.524. If such Protected Information is maintained by Associate in an electronic form or format, Associate must make such Protected Information available to CE in a mutually agreed upon electronic form or format.

g. Amendment of PHI. If Associate maintains Protected Information contained within CE's Designated Record Set, Associate or its agents or Subcontractors shall make such Protected Information available to CE for amendment within ten (10) business days of receipt of a request from CE for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, and shall incorporate any such amendment to enable CE to fulfill its obligations with respect to requests by individuals to amend their PHI under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.526. If any individual requests an amendment of Protected Information directly from Associate or its agents or Subcontractors, Associate must notify CE in writing within five (5) business days of receipt of the request. Any denial of amendment of Protected Information maintained by Associate or its agents or Subcontractors shall be the responsibility of CE.

h. Accounting Rights. Associate and its agents or Subcontractors shall make available to CE, within ten (10) business days of notice by CE, the information required to

provide an accounting of disclosures to enable CE to fulfill its obligations under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.528. In the event that the request for an accounting is delivered directly to Associate or its agents or Subcontractors, Associate shall within five (5) business days of the receipt of the request, forward it to CE in writing. It shall be CE's responsibility to prepare and deliver any such accounting requested. Associate shall not disclose any Protected Information except as set forth in Section 2(b) of this Addendum.

i. Governmental Access to Records. Associate shall keep records and make its internal practices, books and records relating to the use and disclosure of Protected Information available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary"), in a time and manner designated by the Secretary, for purposes of determining CE's or Associate's compliance with the HIPAA Rules. Associate shall provide to CE a copy of any Protected Information that Associate provides to the Secretary concurrently with providing such Protected Information to the Secretary when the Secretary is investigating CE. Associate shall cooperate with the Secretary if the Secretary undertakes an investigation or compliance review of Associate's policies, procedures or practices to determine whether Associate is complying with the HIPAA Rules, and permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including Protected Information, that are pertinent to ascertaining compliance.

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

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

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

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

n. Notification of Breach. During the term of this Contract, Associate shall notify CE within five (5) business days of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of Protected Information and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. Associate shall not initiate notification to affected individuals per the HIPAA Rules without prior

notification and approval of CE. Information provided to CE shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired or disclosed during the breach. Associate shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

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

p. Safeguards During Transmission. Associate shall be responsible for using appropriate safeguards, including encryption of PHI, to maintain and ensure the confidentiality, integrity and security of Protected Information transmitted to CE pursuant to the Contract, in accordance with the standards and requirements of the HIPAA Rules.

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

3. Obligations of CE.

a. Safeguards During Transmission. CE shall be responsible for using appropriate safeguards, including encryption of PHI, to maintain and ensure the confidentiality, integrity and security of Protected Information transmitted pursuant to this Contract, in accordance with the standards and requirements of the HIPAA Rules.

b. Notice of Changes. CE maintains a copy of its Notice of Privacy Practices on its website. CE shall provide Associate with any changes in, or revocation of, permission to use or disclose Protected Information, to the extent that it may affect Associate's permitted or required uses or disclosures. To the extent that it may affect Associate's permitted use or disclosure of

PHI, CE shall notify Associate of any restriction on the use or disclosure of Protected Information that CE has agreed to in accordance with 45 C.F.R. Section 164.522.

4. Termination.

a. Material Breach. In addition to any other provisions in the Contract regarding breach, a breach by Associate of any provision of this Addendum, as determined by CE, shall constitute a material breach of this Contract and shall provide grounds for immediate termination of this Contract by CE pursuant to the provisions of the Contract covering termination for cause, if any. If the Contract contains no express provisions regarding termination for cause, the following terms and conditions shall apply:

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

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

b. Reasonable Steps to Cure Breach. If CE knows of a pattern of activity or practice of Associate that constitutes a material breach or violation of the Associate's obligations under the provisions of this Addendum or another arrangement, then CE shall take reasonable steps to cure such breach or end such violation. If CE's efforts to cure such breach or end such violation are unsuccessful, CE shall terminate the Contract, if feasible. If Associate knows of a pattern of activity or practice of a Subcontractor or agent that constitutes a material breach or violation of the Subcontractor's or agent's obligations under the written agreement between Associate and the Subcontractor or agent, Associate shall take reasonable steps to cure such breach or end such violation, if feasible.

c. Effect of Termination.

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

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

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

6. No Waiver of Immunity. No term or condition of this Contract shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions of the Colorado Governmental Immunity Act, CRS 24-10-101 *et seq*. or the Federal Tort Claims Act, 28 U.S.C. 2671 *et seq*. as applicable, as now in effect or hereafter amended.

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

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

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

10. Amendment.

a. Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of the HIPAA Rules and other applicable laws relating to the confidentiality, integrity, availability and security of PHI. The parties understand and agree that CE must receive satisfactory written assurance from Associate that Associate will adequately safeguard all Protected Information and that it is Associate's responsibility to receive satisfactory written assurances from Associate's Subcontractors and agents. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Addendum embodying written assurances consistent with the standards and requirements of the HIPAA Rules or other applicable laws. CE may terminate this Contract upon thirty (30) days written notice in the event (i) Associate does not promptly enter into negotiations to amend this Contract when requested by CE pursuant to this Section, or (ii) Associate does not enter into an amendment to this Contract providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of the HIPAA Rules.

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

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

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

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

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

15. Signature

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

Contractor Legal Name: _____

Signature of Authorized Officer or Agent: _____

Typed or Printed Name of Authorized Officer or Agent: _____

Title of Authorized Officer or Agent: _____

Date: _____

ATTACHMENT A

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

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

No additional permitted uses.

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

No additional permitted disclosures.

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

No subcontractors.

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

Upon receipt of PHI from the Department.

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

No additional restrictions on Use of Data.

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

No additional terms.