

Attachment A

Non-Disclosure Agreement

State of Alaska

(Note: Do not modify this form)

This Non-Disclosure Agreement (the "Agreement") applies to the **RFI for Medicare Advantage** and is made effective upon signature of the Agreement. The Agreement is between the State of Alaska, Department of Administration, Division of Retirement and Benefits (the "State"), and the company named at the end of this document.

Background Information

- A. State is in the process of seeking information to be provided by Recipient in connection with the provision of group Medicare Advantage plans to large public plans and employers (the "Services") under the self-funded health plan State sponsors for eligible retirees and their dependents (the "Plan").
- B. The data and information that State expects to provide to Recipient for use in reviewing Recipient's response to the RFI regarding the Services is confidential and not public data and the parties desire to enter into a Confidentiality Agreement to set forth their respective duties and obligations regarding State's data and information.

Provisions

In consideration of the foregoing Background Information, which is incorporated by this reference as if fully re-written herein and the mutual covenants and provisions set forth herein, the receipt and sufficiency of which is hereby acknowledged, the parties hereto agree as follows:

Section 1. **Confidential Information**. As used in this Agreement, "Confidential Information" shall mean any and all technical and non-technical information about State, including, but not limited to data and information processed by State in connection with evaluating the Services. The term shall also include all "protected health information" (as defined by 45 C.F.R. § 160.103) and any other personally identifiable information ("PII") regarding any individual who is, or may become, eligible for the State's Plan (including, but not limited to, such Plan's pharmacy benefit). The Recipient hereby agrees to abide by State's determination that such information is Confidential Information and that the same is of a special and unique nature and value, important and material, that it gravely affects the effective and successful conduct of the business and that it may include personal identification information or other information of State or State employees and their dependents that is to be maintained as confidential.

Section 2. **Preservation of Confidentiality**. All Confidential Information (a) supplied by any employee, agent, consultant, or independent contractor of State ("State Representatives") to the Recipient or any employee, agent, officer, director, shareholder, independent contractor or representative of the Recipient (collectively, the "Recipient Representatives"), (b) obtained by the Recipient or any Recipient Representatives from any documents, meetings or telephone conversations with any State Representatives or from books or records of State, (c) obtained by the Recipient or any Recipient Representatives or in any other manner including through hosting the software evaluation on Recipient's website, or (d) jointly or individually developed by State and/or Recipient shall be protected and maintained by the Recipient on a confidential basis and the Recipient shall not use any of the Confidential Information for any purposes (other than as permitted by this Agreement). The Recipient shall refrain from directly or indirectly disclosing any of the Confidential Information to any person, firm, fund, or entity, or knowingly making any Confidential Information available to any others for any use (other than as permitted by this Agreement). Failure to mark any of the Confidential Information as confidential or proprietary shall not affect its status as Confidential Information. In furtherance and not in limitation of the foregoing provisions, the Recipient shall:

- (a) Restrict disclosure of the Confidential Information only to those of the persons as may be absolutely necessary;
- (b) Advise all persons to whom Confidential Information is disclosed of the strict obligations of confidentiality hereunder; and
- (c) Take such steps to protect the confidentiality of the Confidential Information as may be taken to protect the Recipient's own confidential materials, but in no event shall the Recipient use less than a reasonable degree of care.

In addition to the foregoing, Recipient agrees to use reasonable and appropriate administrative, physical and technological safeguards to: (i) prevent use or disclosure of the Confidential Information other than as provided for by this Agreement; and (ii) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Confidential Information. Recipient represents and warrants that it has implemented, and during the term of this Agreement shall maintain, comprehensive written privacy and security policies and procedures and the necessary administrative, technical and physical safeguards appropriate to the size and complexity of Recipient's operations and the nature and scope of its activities.

Section 3. Report of Breach. Recipient shall promptly notify State of a breach of any Confidential Information within forty-eight (48) hours of when Recipient discovers such breach. A breach shall be treated as discovered by Recipient as of the first day on which such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, Recipient Representative or other agent of Recipient. Recipient's notification shall be in writing and, if the Confidential Information is PHI or PII, shall include identification of each individual whose PHI or PII has been, or is reasonably believed by Recipient to have been, subject to the breach. Recipient shall include the following information in its notification of breach to State:

- (a) A description of the breach, including the date of the breach and the date of the discovery of the breach, if known;
- (b) A description of the types of Confidential Information that was involved in the breach (such as whether full name, social security number, date of birth, home address, account number, credit card numbers, diagnosis, disability code or other types of PHI or PII were involved);
- (c) Any steps that individuals should take to protect themselves from potential harm resulting from the breach;
- (d) A description of what Recipient is doing to investigate the breach, to mitigate the harm to individuals and to protect against further breaches; and
- (e) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll free telephone number, an e-mail address, Web site or postal address.

In the event that some of the above listed information is not known by Recipient at the time of notification of State of the breach, Recipient shall provide such information to State as soon as it becomes available to Recipient, but in no event later than thirty (30) days after Recipient discovers such breach. Recipient shall also provide such assistance and further information with regard to the breach to State as reasonably requested by State in order for State to timely meet its notice obligations to individuals, the media, and/or governmental agencies, as applicable, under any law or regulation requiring notification of breaches of PHI or PII.

Section 4. Recipient Representatives. Recipient agrees to ensure that any Recipient Representative to whom it provides Confidential Information agrees in writing to the same restrictions and conditions that apply through this Agreement to Recipient with respect to Confidential Information. Such written agreement shall also require the Recipient Representative to implement reasonable and appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Confidential Information

that it receives. Recipient, and not the State, is solely responsible for Recipient Representatives' uses and disclosures of Confidential Information.

Section 5. Ownership of Information. All information learned or developed pursuant to this Agreement shall be "Confidential Information" as defined in this Agreement and shall be the property of State.

Section 6. Information Not Covered Under This Agreement. This Agreement shall not apply to specific information if:

- (a) The information is or later becomes generally available to the public, except as a result of an unauthorized disclosure by the Recipient or Recipient Representatives;
- (b) State gives its prior written consent to the disclosure of information or the waiver of any provision of this Agreement; or
- (c) The information is disclosed to the Recipient by a third party (except an employee or former employee of Recipient or its affiliates) who is not under a legal restriction not to so disclose such information.

Section 7. Fulfillment of Purpose. When requested by State, the Recipient shall:

- (a) Return all documents, copies of documents, computer records and other means of recording or storing Confidential Information in Recipient's or Recipient Representatives' possession to State within five (5) calendar days or, at Recipient's option, destroy all such items;
- (b) Certify in writing to State that the Recipient has so complied; and
- (c) Not use or disclose the Confidential Information or transact business in any manner based upon the Confidential Information.

Section 8. Representations and Warranties. The Recipient represents, warrants and covenants to State that it is entering into this Agreement with the knowledge that this Agreement (including, specifically, this Section 8 is a substantive and material inducement to State to engage in the evaluation of the Recipient's Services, and that no disclosure would be made to the Recipient or the Representatives by State but for the existence of this Agreement.

Section 9. Indemnification of State. The Recipient shall indemnify and hold State harmless from and against all liability, loss, cost or expense (including attorneys' fees) which State may sustain or incur by reason of the breach of any agreements, representations, warranties or covenants of or relating to Recipient or any of the Recipient Representatives contained in this Agreement or by reason of the enforcement by State of any such agreements, representations, warranties or covenants set forth herein. Without limiting the foregoing, in the event of a breach of PHI or PII or similar breach or wrongful disclosure as defined by an applicable law or regulation requiring notification or other remedial action due to the breach or wrongful disclosure of PHI, PII, or other personal or financial information ("Breach Law") that arose out of or related to Recipient's or Recipient Representatives' acts and omissions, Recipient shall indemnify State against all costs and expenses incurred by State that are associated with complying with the notification requirements under the Breach Law. Such indemnification shall include all costs related to notifying individuals or any other entity required to be notified by Breach Law, any remediation necessitated by the breach, any fines or penalties arising out of the breach, and any other actions required or that are customary in the industry to be taken pursuant to the Breach Law (including, without limitation, credit or identity monitoring for affected individuals).

Section 10. Insurance to be Secured by the Recipient. The Recipient shall maintain professional liability insurance/network security as well as the comprehensive general commercial liability insurance, including coverage to protect against any errors or omissions of the Recipient and Recipient's Representatives, crime/dishonesty

insurance relating to Recipient and Recipient's Representatives and the preserving of the Confidential Information and workers' compensation, if required by applicable law.

Section 11. Term. This Agreement may be terminated by State on five (5) days prior written notice to the Recipient.

Section 12. Survival. The restrictions and obligations under this Agreement shall survive any expiration, termination or cancellation of this Agreement and shall continue to bind Recipient, its successors and assigns.

Section 13. Injunctive Relief. The Recipient agrees that this Agreement is necessary to protect the value of the Confidential Information, and the Recipient covenants that any breach of this Agreement shall result in irreparable damage to State to which State shall have no adequate remedy at law, and the Recipient consents to an injunction by any court of competent jurisdiction in Juneau City and Borough, Alaska in favor of State enjoining any breach of this Agreement without the necessity of posting bond, or if bond is required, the same shall not exceed one hundred dollars, without prejudice to any other right or remedy to which State may be entitled.

Section 14. Governing Law. This Agreement shall be governed by and construed and enforced in accordance with the laws of the State of Alaska (regardless of the laws that might be applicable under principles of conflicts of law) as to all matters, including but not limited to, matters of validity, construction, effect and performance.

Section 15. Gender and Number. Words of any gender shall include the other gender and the neuter. Whenever the singular is used, the same shall include the plural wherever appropriate, and whenever the plural is used, the same shall also include the singular wherever appropriate. Without limiting the generality of the foregoing, the plural form of any term that is defined in the singular shall mean collectively all items so defined and the singular form of any term that is defined in the plural shall mean singly each item so defined.

Section 16. References. All references in this Agreement to particular sections, subsections or articles shall, unless expressly otherwise provided, or unless the context otherwise requires, be deemed to refer to the specific sections or articles in this Agreement. The words "herein", "hereof", "hereunder", "hereinabove" and other words of similar import refer to this Agreement as a whole and not to any particular section, subsection or article hereof. Whenever a party to this Agreement agrees or is under an obligation not to unreasonably withhold its consent or approval to any matter, it shall be construed that such party is obligated not to unreasonably withhold, delay or condition its consent or approval.

Section 17. Illustrative Terms. Whenever the word "including", "includes" or any variation thereof is used herein, such term shall be construed as a term of illustration and not a term of limitation. For example, the term "including" shall be deemed to mean "including, without limitation", and the term "includes" shall be deemed to mean "includes, without limitation".

Section 18. Joint Preparation. This Agreement shall not be construed more strictly against any party because the party or its legal representatives participated in its drafting.

Section 19. Response to Subpoena. Recipient shall promptly notify State if it receives a subpoena or other legal process seeking the disclosure of Confidential Information. Such notification shall be provided in a timeframe that allows State a reasonable amount of time to respond to the subpoena, object to the subpoena, or to otherwise intervene in the action to which the subpoena pertains.

Section 20. Notification of Claims. Recipient shall promptly notify State upon notification or receipt of any civil or criminal claims, demands, causes of action, lawsuits, or governmental enforcement actions arising out of or related to this Agreement or the Confidential Information, regardless of whether State and/or Recipient are named as parties in such claims, demands, causes of action, lawsuits, or enforcement actions.

Section 21. Assistance in Litigation or Administrative Proceedings. Recipient shall make itself and any Recipient Representatives, available to State to testify as witnesses, or otherwise, in the event of litigation or administrative

proceedings being commenced against State based upon a claimed violation of any laws protecting the use or disclosure of the Confidential Information.

Section 22. No Third-Party Beneficiaries. It is the intent of the Parties that this Agreement is to be effective only in regard to their rights and obligations with respect to each other. It is expressly not the intent of the Parties to create any independent rights in any third party or to make any third-party beneficiary of this Agreement and no privity of contract shall exist between third parties and each Party.

Indemnification, Insurance, and HIPAA Requirements - BAA

The contractor shall adhere to the following requirements for handling all “Protected Health Information” (PHI) during the course of this contract. The term PHI has the same meaning given to that term by HIPAA, the HITECH Act, and the Privacy and Security Rule.

The contractor may use or disclose PHI for the following purposes: to provide pharmacy benefit management services to the state. The contractor may use or disclose PHI as required by law, and shall not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the state, except for the specific uses and disclosures set out below.

Permitted uses and disclosures: The contractor may only use and disclose PHI owned by the state that it creates, receives, maintains, or transmits if the use or disclosure is in compliance with each applicable requirement of 45 C.F.R. 164.504(e) of the Privacy Rule or this contract. The additional requirements of Subtitle D of the HITECH Act contained in Public Law 111-5 that relate to privacy and that are made applicable with respect to Covered Entities shall also be applicable to the contractor and are incorporated into this contract.

To the extent that the contractor discloses the state’s PHI to a subcontractor, the contractor must obtain, prior to making any such disclosure: (1) reasonable assurances from the subcontractor that it will agree to the same restrictions, conditions, and requirements that apply to the contractor with respect to such information; and (2) an agreement from the subcontractor to notify the contractor of any breach of unsecured PHI, or security incident, promptly, and in any event within five business days of when it becomes aware of such breach or incident.

Safeguards: 45 C.F.R. 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies, procedures and documentation requirements) shall apply to the contractor in the same manner that such sections apply to the state, and shall be implemented in accordance with HIPAA, the HITECH Act, and the Privacy and Security Rule. The additional requirements of Title XIII of the HITECH Act contained in Public Law 111-5 that relate to security and that are made applicable to Covered Entities shall also apply to the contractor and are incorporated into this contract.

Unless the state agrees in writing that this requirement is infeasible with respect to certain data, the contractor shall secure all paper and electronic PHI by encryption or destruction such that the PHI is rendered unusable, unreadable or indecipherable to unauthorized individuals; or secure paper, film and electronic PHI in a manner that is consistent with guidance issued by the Secretary of the United States Department of Health and Human Services specifying the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals, including the use of standards developed under Section 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by Section 13101 of the HITECH Act contained in Public Law 111-5.

Reporting Unauthorized Disclosures and Breaches: During the term of this contract, the contractor shall notify the state within three business days of discovering: (i) any use or disclosure of PHI not provided for in this agreement, including any use or disclosure of the state’s PHI in violation of any applicable federal or state law; (ii) any security incident of which contractor becomes aware; and/or (iii) any Breach of Unsecured PHI of which it becomes aware. The contractor shall identify for the state the individuals whose unsecured PHI has been, or is reasonably believed to have been, breached so that the state can comply with any notification requirements if necessary. The contractor

shall also indicate whether the PHI subject to the breach; intrusion; or unauthorized acquisition, access, use or disclosure was encrypted or destroyed at the time. The contractor shall take prompt corrective action to cure any deficiencies that result in breaches of security; intrusion; or unauthorized acquisition, access, use, and disclosure. For the purposes of reporting under this provision, a reportable security incident shall not include unsuccessful or inconsequential incidents that do not represent a material threat to the confidentiality, integrity or availability of PHI (such as scans, pings or unsuccessful attempts to penetrate computer networks).

If the unauthorized acquisition, access, use or disclosure of the state's PHI involves only secured PHI, the contractor shall notify the state within 10 days of discovering the breach but is not required to notify the state of the names of the individuals affected.

Contractor's Agents: If the contractor uses a subcontractor or agent to provide services under this contract, and the subcontractor or agent creates, receives, maintains, or transmits the state's PHI, the subcontractor or agent shall sign an agreement with the contractor containing substantially the same provisions as this Appendix. Contractor will indemnify the state in the event of any violation of the subcontractor or agent agreement. The contractor shall mitigate the effects of any violation of that agreement. Contractor is responsible for all subcontractor or agent's breach of the terms of this agreement, and for all acts or omissions of its subcontractors or agents with respect to the services provided to the State.

Availability of Information to the State: Within 15 days after the date of a written request by the state, the contractor shall provide any information necessary to fulfill the state's obligations to provide access to PHI under HIPAA, the HITECH Act, or the Privacy and Security Rule.

Accountability of Disclosures: If the contractor is required by HIPAA, the HITECH Act, or the Privacy or Security Rule to document a disclosure of PHI, the contractor shall make that documentation. If the state is required to document a disclosure of PHI made by the contractor, the contractor shall assist the state in documenting disclosures of PHI made by the contractor so that the state may respond to a request for an accounting in accordance with HIPAA, the HITECH Act, and the Privacy and Security Rule. Accounting records shall include the date of the disclosure, the name and if known, the address of the recipient of the PHI, the name of the individual who is subject of the PHI, a brief description of the PHI disclosed and the purpose of the disclosure. Within 15 days of a written request by the state, the contractor shall make the accounting record available to the state.

Amendment of PHI: Within 30 days of a written request by the state or an individual, the contractor shall amend PHI maintained, transmitted, created or received by the contractor on behalf of the state as directed by the state or the individual when required by HIPAA, the HITECH Act or the Privacy and Security Rule, or take other measures as necessary to satisfy the state's obligations under 45 C.F.R. 164.526.

Internal Practices: The contractor shall make its internal practices, books and records relating to the use and disclosure of the state's PHI available to the state and all appropriate federal agencies to determine the state's and the contractor's compliance with HIPAA, the HITECH Act and the Privacy and Security Rule. To the extent the contractor is to carry out one or more of state's obligations under Subpart E of 45 C.F.R. Part 164, the contractor must comply with the requirements of that Subpart that apply to the state in the performance of such obligations.

Breach: A breach of a material term of this Appendix by the contractor that is not cured within a reasonable period of time may be grounds for the immediate termination of the contract.

Effect of Termination: Upon termination of the contract, the contractor will, at the direction of the state, either return or destroy all PHI received from the state or created, maintained, or transmitted on the state's behalf by the contractor in any form. Unless otherwise directed, the contractor is prohibited from retaining any copies of PHI received from the state or created, maintained, or transmitted by the contractor on behalf of the state. If destruction or return of PHI is not feasible, the contractor must continue to extend the protections of this Appendix to PHI and

limit the further use and disclosure of the PHI. The obligations in this Appendix shall continue until all of the PHI provided by the state to the contractor is either destroyed or returned to the state.

Agree Disagree **I have read and agree to the terms of this Agreement, and represent and warrant that I have authority to bind this entity named below to these terms and conditions.**

Printed Name of Authorized Representative _____

Title _____

Signature _____

Date _____

Contractor Name _____