State of Alaska Department of Health
Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
Business Associate Agreement

This HIPAA Business Associate Agreement is between the Department of Health (hereafter known as **Covered Entity or CE)** and _____
(hereafter known as **Business Associate or BA**). This agreement is intended to accomplish the objectives of a HIPAA Business Associate Agreement ("BAA") as set out in 45 C.F.R. §164.504(e)(3)(i).

PART 1: Business Associate Agreement (BAA)

RECITALS

Whereas,

A. CE wishes to disclose certain information to BA, some of which may constitute Protected Health Information ("PHI");

B. It is the goal of CE and BA to protect the privacy and provide for the security of PHI owned by CE that is disclosed to BA or accessed, received, stored, maintained, modified or retained by BA in compliance with HIPAA (42 U.S.C. 1320d – 3120d-8) and its implementing regulations at 45 C.F.R. 160 and 45 C.F.R. 164 (the "Privacy and Security Rule"), the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5) (the "HITECH Act"), and with other applicable laws;

C. The purpose and goal of the HIPAA Business Associate Agreement ("BAA") is to satisfy certain standards and requirements of HIPAA, HITECH Act, and the Privacy and Security Rule, including but not limited to 45 C.F.R. 164.502(e) and 45 C.F.R. 164.504(e), as may be amended from time to time;

D. CE may operate a drug and alcohol treatment program that must comply with the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law and regulations, 42 U.S.C. 290dd-2 and 42 C.F.R. Part 2 (collectively "Part 2"); and

E. BA may be a Qualified Service Organization ("QSO") under Part 2 and therefore must agree to certain mandatory provisions regarding the use and disclosure of substance abuse treatment information.

Therefore, in consideration of mutual promises below and the exchange of information pursuant to the BAA, CE and BA agree as follows:

1. Definitions.

   a. General: As used in this BAA, the terms "Protected Health Information," "Health Care Operations," and other capitalized terms have the same meaning given to those terms by HIPAA, the HITECH Act and the Privacy and Security Rule. In the event of any conflict between the mandatory provisions of HIPAA, the HITECH Act or the Privacy and Security Rule, and the provisions of this BAA, HIPAA, the HITECH Act or the Privacy and Security Rule shall control. Where the provisions of this BAA differ from those mandated by HIPAA, the HITECH Act or the

Privacy and Security Rule but are nonetheless permitted by HIPAA, the HITECH Act or the Privacy and Security Rule, the provisions of the BAA shall control.

b. Specific:

1) Business Associate: "Business Associate" or "BA" shall generally have the same meaning as the term "business associate" at 45 C.F.R. 160.103.

2) Covered Entity: "Covered Entity" or "CE" shall have the same meaning as the term "covered entity" at 45 C.F.R. 160.103.

3) Privacy and Security Rule: "Privacy and Security Rule" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.

4) Triennially: "Triennially" shall mean once every three years.

2. Statement of Work and Responsibilities.

As provided by AS 44.21.020 and AS 44.21.160, The BA provides automatic data processing services to the CE. These services include storage, transmission, security, and recovery of electronic information owned by CE. BA is responsible for ensuring continuity of service, delivery, and access to CE electronic information at all times including in the event of a disaster.

3. Permitted Uses and Disclosures by Business Associate.

a. BA may only use or disclose PHI for the following purposes:
1) BA may use or disclose PHI as required by law.

2) BA agrees to make uses and disclosures and requests for PHI consistent with CE's minimum necessary policies and procedures.

3) BA may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by CE, except for the specific uses and disclosures set out below.

4) BA may disclose PHI for the proper management and administration of BA or to carry out the legal responsibilities of BA, provided the disclosures are required by law, or BA obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notified BA of any instances of which it is aware in which the confidentiality of the information has been breached.

5) BA may provide data aggregation services related to the health care operations of CE.

4. Obligations of Business Associate.

a. Permitted uses and disclosures: BA may only use and disclose PHI owned by the CE 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 BAA. 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 BA and are incorporated into this BAA.

To the extent that BA discloses CE's PHI to a subcontractor, BA 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 BA with respect to such information; and (2) an agreement from the subcontractor to notify BA of any Breach of confidentiality, or security incident, within three business days of when it becomes aware of such Breach or incident.

b. 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 BA in the same manner that such sections apply to CE, 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 BA and are incorporated into this BAA.

Unless CE agrees in writing that this requirement is infeasible with respect to certain data, BA 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.

BA shall patch its operating systems and all applications within two weeks of the release of any patch. BA shall keep its antivirus and antimalware installed and active. BA shall limit its use of administrative accounts for necessary IT operations only.

c. Reporting Unauthorized Disclosures and Breaches: During the term of this BAA, BA shall notify CE within 72 hours of discovering a Breach of security; intrusion; or unauthorized acquisition, access, use or disclosure of CE's PHI in violation of any applicable federal or state law, including security incidents. BA shall identify for the CE the individuals whose unsecured PHI has been, or is reasonably believed to have been, breached so that CE can comply with any notification requirements if necessary. BA 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. BA shall take prompt corrective action to cure any deficiencies that result in Breaches of security; intrusion; or unauthorized acquisition, access, use, and disclosure. BA shall fulfill all breach notice requirements unless CE notifies BA that CE will take over the notice requirements. BA shall reimburse CE for all costs incurred by CE that are associated with any mitigation, investigation and notice of Breach CE undertakes or provides under HIPAA, HITECH Act, and the Privacy and Security Rule as a result of a Breach of CE's PHI caused by BA or BA's subcontractor or agent.

If the unauthorized acquisition, access, use or disclosure of CE's PHI involves only Secured PHI, BA shall notify CE within 10 days of discovering the Breach but is not required to notify CE of the names of the individuals affected.

d. BA is not an agent of CE.

e. BA's Agents: If BA uses a subcontractor or agent to provide services under this BAA, and the subcontractor or agent creates, receives, maintains, or transmits CE's PHI, the subcontractor or agent shall sign an agreement with BA containing substantially the same provisions as this BAA and further identifying CE as a third-party beneficiary with rights of enforcement and indemnification from the subcontractor or agent in the event of any violation of the subcontractor or agent agreement. BA shall mitigate the effects of any violation of that agreement.

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

g. Accountability of Disclosures: If BA is required by HIPAA, the HITECH Act, or the Privacy or Security Rule to document a disclosure of PHI, BA shall make that documentation. If CE is required to document a disclosure of PHI made by BA, BA shall assist CE in documenting disclosures of PHI made by BA so that CE 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 CE, BA shall make the accounting record available to CE.

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

i. Internal Practices: BA shall make its internal practices, books and records relating to the use and disclosure of CE's PHI available to CE and all appropriate federal agencies to determine CE's and BA's compliance with HIPAA, the HITECH Act and the Privacy and Security Rule.

j. Risk Assessment: Upon agreement execution and triennially thereafter, or upon changes that occur which significantly affect the security posture of the system (whichever comes first), BA shall comply and complete CE's security assessment. Upon receipt of the security assessment, CE will review BA's responses prior to granting authority to operate, and provide any necessary instruction to ensure the confidentiality, integrity, and availability of CE's PHI. BA shall triennially, or upon changes that occur which significantly affect the security posture of the system (whichever comes first), review and update CE security assessment, as required, in order to comply with BA's current system controls. BA must provide an implementation response for each specific system control. Upon receipt of the updated assessment, CE will review the changes to the system for renewal of authority to operate.

k. To the extent BA is to carry out one or more of CE's obligations under Subpart E of 45 C.F.R. Part 164, BA must comply with the requirements of that Subpart that apply to CE in the performance of such obligations.

l. Audits, Inspection and Enforcement: CE may, after providing 10 days' notice to the BA, conduct an inspection of the facilities, systems, books, logs, and records of BA that relate to BA's use of CE's PHI, including inspecting logs showing the creation, modification, viewing, and deleting of PHI at BA's level. Failure by CE to inspect does not waive any rights of the CE or relieve BA of its responsibility to comply with this BAA. CE's failure to detect or failure to require remediation does not constitute acceptance of any practice or waive any rights of CE to enforce this BAA.

m. Restrictions and Confidential Communications: Within 10 business days of notice by CE of a restriction upon use or disclosure or request for confidential communications pursuant to 45 C.F.R.164.522, BA shall restrict the use or disclosure of an individual's PHI. BA may not respond directly to an individual's request to restrict the use or disclosure of PHI or to send all communication of PHI to an alternate address. BA shall 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 the BA.

n. Indemnification: BA shall indemnify and hold harmless CE for any civil or criminal monetary penalty or fine imposed on CE for acts or omissions in violation of HIPAA, the HITECH Act, or the Privacy or Security Rule that are committed by BA, a member of its workforce, its agent, or its subcontractor.

5. Obligations of CE. CE will be responsible for using legally appropriate safeguards to maintain and ensure the confidentiality, privacy and security of PHI transmitted to BA under the BAA until the PHI is received by BA. CE will not request BA to use or disclose PHI in any manner that would not be permissible under HIPAA, the HITECH Act or the Privacy and Security Rule if done by CE.

6. Termination.

a. Breach: A breach of a material term of the BAA by BA that is not cured within a reasonable period of time will provide grounds for the immediate termination of the contract.

b. Reasonable Steps to Cure: In accordance with 45 C.F.R. 164.504(e)(1)(ii), CE and BA agree that, if it knows of a pattern of activity or practice of the other party that constitutes a material breach or violation of the other party's obligation under the BAA, the nonbreaching party will take reasonable steps to get the breaching party to cure the breach or end the violation and, if the steps taken are unsuccessful, terminate the BAA if feasible, and if not feasible, report the problem to the Secretary of the U.S. Department of Health and Human Services.

c. Effect of Termination: Upon termination of the contract, BA will, at the direction of the CE, either return or destroy all PHI received from CE or created, maintained, or transmitted on CE's behalf by BA in any form. Unless otherwise directed, BA is prohibited from retaining any copies of PHI received from CE or created, maintained, or transmitted by BA on behalf of CE. If destruction or return of PHI is not feasible, BA must continue to extend the protections of this BAA to PHI and limit the further use and disclosure of the PHI. The obligations in this BAA shall continue until all of the PHI provided by CE to BA is either destroyed or returned to CE.

7. Amendment. The parties acknowledge that state and federal laws relating to electronic data security and privacy are evolving, and that the parties may be required to further amend this BAA to ensure compliance with applicable changes in law. Upon receipt of a notification from CE that an applicable change in law affecting this BAA has occurred, BA will promptly agree to enter into negotiations with CE to amend this BAA to ensure compliance with changes in law.

8. Ownership of PHI. For purposes of this BAA, CE owns the data that contains the PHI it transmits to BA or that BA receives, creates, maintains, or transmits on behalf of CE.

9. Litigation Assistance. Except when it would constitute a direct conflict of interest for BA, BA will make itself available to assist CE in any administrative or judicial proceeding by testifying as witness as to an alleged violation of HIPAA, the HITECH Act, the Privacy or Security Rule, or other law relating to security or privacy.

10. Regulatory References. Any reference in this BAA to federal or state law means the section that is in effect or as amended.

11. Interpretation. This BAA shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy and Security Rule and applicable state and federal laws. The parties agree that any ambiguity in BAA will be resolved in favor of a meaning that permits the CE to comply with and be consistent with HIPAA, the HITECH Act, and the Privacy and Security Rule. The parties further agree that where this BAA conflicts with a contemporaneously executed confidentiality agreement between the parties, this BAA controls.

12. No Private Right of Action Created. This BAA does not create any right of action or benefits for individuals whose PHI is disclosed in violation of HIPAA, the HITECH Act, the Privacy and Security Rule or other law relating to security or privacy.

13. Privacy and Security Point of Contact. All communications occurring because of this BAA shall be sent to doh.its.dso@alaska.gov in addition to the CE.

NOTE: No adjustments are permitted to Part II or Part III of this agreement

PART II: State of Alaska, Department of Health HIPAA and HITECH Information Security Agreement (ISA)

This agreement, effective upon the date of full contract execution, is in accordance with **Covered Entity's (CE)** obligations under:

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the applicable requirements of HIPAA's implementing regulations issued by the U.S. Department of Health and Human Services (HHS), Title 45 of the Code of Federal Regulations ("CFR") Parts 160-164 ("HIPAA Regulations");
- The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), as incorporated in the American Recovery and Reinvestment Act of 2009, Public Law 111-005;
- The Genetic Information Nondiscrimination Act ("GINA");
- The HIPAA Final Rule (the "Final Rule").

Covered Entity (CE) and **Business Associate (BA)** acknowledge and agree to the terms and conditions of this agreement to ensure the confidentiality, integrity, and availability of Protected Health Information by lawfully complying with the aforementioned provisions and regulations, all as amended from time to time.

1. Definitions.

    a. Breach: shall mean the impermissible acquisition, access, use, or disclosure of Protected Health Information (PHI) which compromises the security, confidentiality, privacy, or integrity of such information pursuant to the HITECH Act § 13400, any regulations issued thereunder, or as amended by law. An impermissible use or disclosure of PHI is presumed to be a breach unless the CE or BA, as applicable, demonstrates that there is a low probability, as stipulated in 45 CFR 164.402, that the PHI has been compromised. This does not include:

        1) Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or BA, if access was in good faith and within the scope of authority; or

        2) Inadvertent disclosure by a person authorized to access the PHI to another person authorized to access the PHI.

    b. Business Associate: shall mean an individual or entity who or which performs a function or activity on behalf of, or provides a service, to CE that involves the creation, use, or disclosure of PHI. Shall have the meaning given to such term under the HIPAA Privacy Rule, the HIPAA Security Rule, and the HITECH Act, but not limited to, Section 13400 and Section 13401 of the HITECH Act, 42 U.S.C. § 17938 and 45 CFR 160.103.

    c. Covered Entity: shall mean a health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered under the HIPAA Regulations. CE shall have the meaning given to such term under the HIPAA Privacy Rule and the HIPAA Security Rule, including but not limited to, 45 CFR 160.103.

    d. Data Aggregation: shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 CFR 164.501.

    e. Data Breach Notification Rule: shall mean the standards for Breach Notification of Unsecured Protected Health Information at 45 CFR part 164, subpart D, as amended.

    f. Designated Record Set: shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 CFR 164.501.

    g. Electronic Protected Health Information (ePHI): shall mean PHI maintained or transmitted in electronic form.

    h. Health Care Operations: shall have the meaning as defined under the HIPAA Rules, including, but not limited to, 45 CFR 164.501.

    i. Individual: shall have the meaning as defined in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

j. Limited Data Set: shall mean PHI that excludes direct identifiers of the individual or of relatives, employers, or household members of the individual. (See 45 CFR 164.514(e)(2)).

k. Minimum Necessary: BA shall only request, use, and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use, or disclosure.

l. Personally Identifiable Information (PII): as defined in OMB Memorandum M-07-16 refers to "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or associated with a specific individual." The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified.

m. Privacy Official: shall mean the CE's designated individual, and such individual's designees, who are responsible for the development and implementation of CE's policies and procedures regarding privacy and confidentiality of PHI.

n. Protected Health Information (PHI): shall mean either medical information or personally identifiable information in electronic, physical, or oral form. Medical information is any information in possession of, or derived from, a physician or other provider of health care, or a health care service plan regarding an individual's medical history, mental or physical condition, or treatment. PHI shall have the meaning given to such term under the HIPAA Privacy Rule and the GINA, including, but not limited to 45 CFR 160.103.

o. Required by law: shall have the meaning given to such term as stated within 45 CFR 164.103.

p. Security Incident: shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system that is created, received, maintained, or transmitted by or on behalf of CE. (See 45 CFR 164.304).

q. Unsecured PHI: shall mean PHI that is not secured in accordance with guidance issued by the United States Department of Health and Human Services (HHS) under the HITECH Act including, but not limited to, 42 U.S.C. § 17932(h), and applicable regulations issued thereunder.

2. Privacy and Security of PHI

a. Permitted Uses and Disclosures. BA is permitted or required to use or disclose PHI it creates, receives, maintains, or transmits in service to CE only as follows:

1) Functions and Activities on Covered Entity's Behalf. BA is permitted to use and disclose the minimum necessary PHI it creates, receives, maintains, or transmits to/from CE, to perform those services set forth in the underlying contract, provided that no such use or disclosure would violate HIPAA Regulations, or the HITECH Act and applicable regulations issued thereunder, if CE itself made the use or disclosure.

2) Marketing and Fundraising. Unless expressly authorized by the underlying contract between the parties, BA shall not Use or Disclose PHI for any marketing or fundraising purpose.

3) Audit. For purposes of determining BA's compliance with HIPAA, upon request of CE or the Secretary of HHS, BA shall:

   - Make its HIPAA policies and procedures, related documentation, records maintained, and any other relevant internal practices, books, and records relating to the use and disclosure of PHI, available to the Secretary of HHS or to CE.

   - Provide reasonable access to BA's facilities, equipment, hardware, and software used for the maintenance or processing of CE's PHI.

4) Record Keeping. BA agrees to implement appropriate record keeping procedures to enable it to comply, and to adequately evidence such compliance, including; the documentation required regarding subcontractors and agents, records of BA's workforce HIPAA education and training, documentation related to any breach, Business Associate Agreements issued to third parties with whom BA discloses PHI for BA's proper management and administration, or as required by law.

5) Business Associate's Operations. BA may use and disclose the PHI it creates, receives, maintains, or transmits in service to CE, as necessary, to perform the BA's obligations under the contract, to enable that BA's proper management and administration of CE's PHI, or to carry out BA's legal responsibilities. All PHI disclosures must maintain compliance with the HIPAA minimum necessary standard.

3. Prohibition on Unauthorized Use or Disclosure. BA shall neither use nor disclose PHI it creates, receives, maintains, or transmits in service to CE, except as permitted or required by the contract, as required by law, or as otherwise permitted in writing by CE. BA acknowledges that BA will be liable for violating any of the requirements of this agreement relating to the use or disclosure of PHI, or any privacy-related requirements of the HITECH Act and regulations issued thereunder.

4. Offshoring Prohibition. BA may not transmit, store, process, or make PHI accessible to any recipient outside the United States of America without CE's prior written consent.

5. Compliance with Laws; Regulatory Amendments. BA shall comply with all applicable state and federal privacy and security laws pursuant to HIPAA, HIPAA Regulations, the HITECH Act, and any regulations promulgated thereunder. Any regulations or amendments to applicable privacy and security laws shall be automatically included in this agreement, such that this agreement remains in compliance with such regulations or amendments. Any future state privacy and security laws shall be automatically included in this agreement, such that this agreement remains in compliance with such regulations or amendments.

6. Effect. The terms and provisions of this agreement shall supersede any other conflicting or inconsistent terms and provisions in any other contract between the parties, including any exhibits, attachments, addenda, or amendments thereto, and any other documents incorporated by reference therein, which pertain or relate to the use or disclosure of PHI by either party, or the creation or receipt of PHI by BA on behalf of CE.

7. Change in Law Amendments. The parties agree to amend this agreement to the extent necessary to allow either party to comply with any amendments to any provision of HIPAA or its implementing regulations or any judicial, legislative, or administrative interpretation which alters or conflicts with any provisions contained herein.

8. Definitions, Construction of Terms, and Interpretation. Capitalized terms herein without definition shall have the same meanings assigned to such terms in 45 CFR Parts 160 and 164. The terms of this agreement shall be construed in light of any applicable interpretation or guidance on HIPAA and/or the Privacy and Security Standards issued by HHS or the Office for Civil Rights from time to time. This agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA and the Privacy and Security Standards. The parties agree that any ambiguity in this agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the Privacy and Security Standards.

9. No Third-Party Beneficiaries. Nothing in this agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

10. Independent Contractors. The parties agree that they are independent parties and not employees, partners, or party to a joint venture of any kind. Neither party shall hold itself out as the other's agent for any purpose and shall have no authority to bind the other to any obligation.

11. Information Safeguards. BA shall develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards, in compliance with applicable state and federal laws, to preserve the integrity, confidentiality, and availability of PHI, and to prevent unauthorized disclosures of PHI created or received for or from CE as required by 45 CFR Part 164, Subpart C, the HITECH Act, HHS' guidance on the Direct Liability of Business Associates, and any applicable regulations issued thereunder. BA shall document and keep such safeguards current and shall develop and implement policies and procedures to meet the Security Rule documentation requirements of the HITECH Act and shall, upon CE's request, either orally or in writing, provide CE with a copy of its policies and procedures related to such safeguards. BA shall also provide reasonable description of the practices and processes that are in place to support the policies, procedures, and requirements.

    a. 45 CFR 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies, procedures, and documentation requirements) shall apply to BA in the same manner that such sections apply to CE 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 CE shall also apply to BA and are incorporated into this Information Security Agreement.

12. Subcontractors and Agents. BA shall require any of its subcontractors and agents to which BA is permitted by this agreement or in writing by CE to disclose PHI, to sign a further Business Associate Agreement and to provide reasonable assurance evidenced by written contract, that such subcontractor or agent shall comply with the same privacy and security safeguard obligations with respect to PHI that are applicable to BA under this agreement, including, but not limited to:

    a. Holding such PHI in confidence and using or further disclosing it only for the purpose for which BA disclosed it to the agent, subcontractor, or other third party, or as required by law.

    b. In compliance with 45 CFR 164.400-414 Subcontractor or Agent shall provide notification to BA, and the BA shall provide notification to the CE, of any instance of which the agent, subcontractor, or other third party becomes aware in which the confidentiality of such PHI was breached.

13. Minimum Necessary and Limited Data Set. BA's use, disclosure, or request of PHI shall utilize a limited data set, whenever possible. Otherwise, BA shall, in its performance of the functions, activities, services, and operations specified in Section B.1 above, make reasonable efforts to use, to disclose, and to request only the minimum amount of PHI reasonably necessary to accomplish the intended purpose of the use, disclosure, or request, except that BA shall not be obligated to comply with the minimum necessary limitations with respect to those exceptions specified in 45 CFR 164.502 (b)(2). BA shall comply with the requirements governing the minimum necessary use and disclosure of PHI set forth in the HITECH Act § 13405(b) and any applicable regulations or other guidance issued thereunder.

14. Employee Education. BA shall inform all of its employees, workforce members, subcontractors, and agents ("BA Personnel"), whose services may be used to satisfy BA's obligations under the agreement, of the BA's obligations under this agreement. BA represents and warrants that the BA Personnel are under legal obligation to BA, by contract or otherwise, sufficient to enable BA to fully comply with the provisions of this agreement. BA will maintain a system of sanctions for any BA Personnel who violates this agreement. (See 45 CFR 164.316).

15. Risk Assessment. Upon agreement execution, and prior to any system entering a production state or containing production data, BA must complete CE's established security assessment process and obtain Authority to Operate (ATO). Any identified risks must be remediated to ensure that the system complies with the CE's security standards and the CE's selected standards for HIPAA compliance. This security assessment process must be completed triennially thereafter, or upon changes that occur which significantly affect the security posture of the system (whichever comes first), and Authority to Operate must be obtained, reflecting the current risk profile of the system.

16. PHI Access, Amendment, Restriction, and Reporting

    a. Access. BA shall, upon CE's reasonable request, and in compliance with 45 CFR 164.524(b)(2)(i), permit an individual (or the individual's personal representative) to obtain and inspect copies of any PHI about the individual which BA created or received for or from CE and that is in BA's custody or control. BA shall provide such information in an electronic format, if requested by the individual, and as directed by CE.

    b. Amendment. BA shall, upon receipt of notice from CE, promptly amend or permit CE access to amend, any portion of an individual's PHI which BA created or received for or from CE and that is in BA's custody or control.

    c. Restriction. BA shall, upon CE's written notice of any changes in, or restrictions to, the permitted use or disclosure of PHI, promptly restrict the use or disclosure of PHI consistent with the CE's instructions. CE will promptly notify BA in writing of the termination of any such restriction agreement and, with respect to termination of any such restriction agreement, instruct BA as to whether any PHI will remain subject to the terms of the restriction agreement.

    d. Reporting

        1) Legal or Authorized Disclosure Reporting. Except as permitted by applicable law, BA shall document each disclosure it makes of an individual's PHI to a third party. Such report shall include the affected individual's name, the person or entity to whom the PHI was disclosed, what was disclosed, why the information was disclosed, the date of such disclosure and any other information necessary for CE to comply with relevant statutes and regulations. The

report shall be furnished to CE within fifteen (15) calendar days of its request. In addition, where BA is contacted directly by an individual based on information provided to the individual by CE, and where so required by the HITECH Act and/or any accompanying regulations, BA shall make such report available directly to the individual.

- ***Disclosure Accounting.*** Upon request, BA shall forward to CE a report of disclosures as required by 45 CFR 164.528, and as applicable, the HITECH Act § 13405(c) and any regulations issued thereunder.

- ***Disclosure Accounting Retention.*** BA shall maintain an accounting of such disclosures for six (6) years after the date of occurrence.

2) Security Incident Reporting**.** BA shall report to CE's Chief Privacy Officer and Chief Information Security Officer as stipulated in 45 CFR 164 after BA knows, or should reasonably have known of such Security Incident, any Security Incident of which BA becomes aware. In addition, BA shall, upon CE's request, report any attempted unauthorized access, use, disclosure, modification, or destruction of ePHI. If any such security incident resulted in a disclosure of PHI not permitted by this agreement, BA shall make a report in accordance with Section C.5, below. If BA is aware of a pattern of activity or practice by its subcontractor that constitutes a breach or violation of the subcontractor's obligations under its Business Associate Agreement or obligations with BA, BA must take reasonable steps to cure the breach or end the violation and take further actions consistent with 45 CFR 164.504.

- Breach Reporting. BA shall report to CE any breaches of PHI as stipulated in 45 CFR 164. BA shall make such report to CE's Privacy Officer after BA knows, or should reasonably have known, of such breach. BA shall cooperate with CE in investigating such breach, and in meeting CE's obligations under the HITECH Act and any other security breach notification laws. BA shall report all breaches to CE in writing (and in the format requested by CE) and such reports shall, at a minimum:

    - Identify the nature of the breach, including the date of the breach and the date of discovery of the breach.
    - Identify which elements of the PHI (e.g., full name, social security number, date of birth, etc.) were breached, or were part of the breach.
    - Identify who was responsible for the breach and who received the PHI.
    - Identify what corrective actions BA took or will take to prevent further incidents of a breach.
    - Identify what BA did or will do to mitigate any deleterious effect of the breach.
    - Identify BA contact information and procedures to enable CE to obtain additional information if required.
    - Provide such other information, including a written report, as CE may reasonably request.

e. Obligations in the Event of an Improper Pattern of Activity or Practice. In the event that either party becomes aware of a pattern of activity or practice of the other party that constitutes a material breach or violation of this agreement, the party discovering such pattern of activity or practice must take reasonable steps to cause the other party to cure the breach or end the violation. If a cure is not effectuated within a reasonable time period, specified by the party requesting the cure, such party shall terminate the contract, if feasible, or if not feasible report the problem to the Secretary of HHS or its designee. (See 45 CFR 164.504(e)(1)(ii) and HITECH Act § 13404(b)).

17. Inspection of Books and Records. BA shall make available for inspection its internal practices, books, and records (relating to its use and disclosure of the PHI it creates for, or receives from, CE) to CE and/or the HHS to determine compliance with the HIPAA Regulations or the BA's compliance with this agreement. (See 45 CFR 164.504(e)(2)(ii).

18. Designated Record Set. BA agrees that all PHI received by or created for CE shall be included in an individual's Designated Record Set. BA shall maintain such Designated Record Set with respect to services provided to an individual under this agreement and shall allow such individual to access the Designated Record Set as provided in the HIPAA Regulations.

19. Restriction Contracts and Confidential Communications. BA shall comply with any agreement that CE makes that either; (i) restricts use or disclosure of PHI pursuant to 45 CFR 164.522(a); or (ii) requires confidential communication about PHI pursuant to 45 CFR 164.522(b), provided that CE notifies BA, in writing, of the restriction or confidential communication obligations that BA must follow. CE will promptly notify BA in writing of the termination of any such restriction agreement or confidential communication requirement, and with respect to termination of any such restriction agreement, instruct BA whether any PHI will remain subject to the terms of the restriction agreement.

20. Termination and Continuing Privacy and Security Obligations

    a. Termination of Contract. As required by the HIPAA Regulations and this agreement, CE may, in addition to other available remedies, terminate the contract if BA has materially breached any provision of this agreement and has failed to cure or take actions to cure such material breach within five (5) calendar days of such breach. CE shall exercise this right to terminate the contract by providing BA written notice of termination, which shall include the reason for the termination. Any such termination shall be effective immediately or at such other date specified in CE's notice of termination. Within thirty (30) calendar days of such termination of the contract, BA shall provide to CE one final report of any and all breaches made of all individuals' PHI during the term of the contract.

        1) Obligations upon Termination. Upon termination, cancellation, expiration, or other conclusion of the contract, BA shall:

            - As directed by CE, BA shall immediately return or destroy all PHI, including all copies of and any data or compilations derived from, and allowing identification of, any individual who is a subject of the PHI, in whatever form or medium (including in any electronic medium under BA's custody or control), and at whatever location the PHI resides including offices local and remote, data centers,

remote storage facilities, off-site backup facilities and vendors, and all other locations, that BA created or received for or from CE. Returned PHI must be provided to the CE in a common, nonproprietary, industry standard data format.

- Complete all such return or destruction activities as promptly as possible, but no later than thirty (30) calendar days after the effective date of the termination, cancellation, expiration, or other conclusion of the contract.

- These provisions shall apply to PHI that is in the possession of subcontractors or agents of BA.

2) Continuing Privacy and Security Obligation. BA's obligation to protect the privacy and security of the PHI, including all copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the PHI it created for or received from CE, shall be continuous and survive termination, cancellation, expiration, or other conclusion of the contract.

3) Termination for Cause. Without limiting the termination rights of the parties pursuant to the contract and upon CE's knowledge of a material breach of this contract by BA, CE shall either:

    - Provide an opportunity for BA to cure the breach or end the violation and, if BA does not cure the breach or end the violation within the time specified by CE, terminate the contract, if feasible; or

    - Immediately terminate the contract if cure is not possible, if feasible.

4) Effect of Termination.

    - Except as provided in paragraph (2) of this Section, upon termination of the contract for any reason, as directed by CE, BA shall promptly return or destroy all PHI received from or created or received by BA on behalf of, CE that BA maintains in any form and retain no copies. This provision shall apply to PHI that is in the possession of subcontractors or agents of BA. Returned PHI must be provided to the CE in a common, nonproprietary, industry standard data format.

    - In the event that BA reasonably believes that returning or destroying the PHI is infeasible, BA shall provide to CE prompt notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return, or destruction is infeasible, BA shall extend the protections of the contract to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as BA maintains such PHI.

21. Conflicts

The terms and conditions of this agreement shall prevail in the event any terms and conditions herein conflict with any provision of the contract.

Privacy and Security Contact Information

1. **Privacy**
   a. **Covered Entity**
      i. E-mail: privacyofficial@alaska.gov
   b. **Business Associate**
      i. Attn: _____
      ii. Phone: _____
      iii. E-mail: _____
2. **Security**
   a. **Covered Entity**
      i. E-mail: doh.its.dso@alaska.gov
   b. **Business Associate**
      i. Attn: _____
      ii. Phone: _____
      iii. E-mail: _____

PART III: Resolution of Conflicts Between BAA and ISA

The terms and conditions of **PART II: State of Alaska, Department of Health HIPAA and HITECH Information Security Agreement (ISA)** in this agreement shall prevail in the event any terms and conditions herein conflict with any provision of **PART 1: Business Associate Agreement (BAA).**

In witness thereof, the parties hereto have duly executed this agreement as of the effective date.