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).

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; including, but not limited to:

    1. The Genetic Information Nondiscrimination Act ("GINA");

    2. The HIPAA Final Rule (the "Final Rule").

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:

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

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

iii) 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.

iv) 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 or created on behalf of 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.

Notwithstanding the foregoing, if the Business Associate does not handle ePHI in connection with its services to the Covered Entity, the obligations described above regarding electronic data processing, transmission, and disaster recovery shall not apply.

3) Permitted Uses and Disclosures by Business Associate.

a) BA may only use or disclose PHI for the following purposes:

i) BA may use or disclose PHI as required by law.

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

iii) 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.

iv) 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.

v) 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.

BA is permitted or required to use or disclose PHI it creates, receives, maintains, or transmits in service to CE as follows:

i) 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.

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

(1) 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.

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

iii) 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.

iv) 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.

b) 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.

c) 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.

d) 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.

e) 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.

f) 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.

g) 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.

h) 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.

Breach Reporting. BA shall report to CE any breaches of PHI as stipulated in 45 CFR 164.410. BA shall make such report to CE's Privacy Official within 72 hours of discovery. 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, and such reports shall include, at a minimum:

i) Identify the nature of the breach, including the occurrence and the discovery dates.

ii) 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.

iii) Identify who was responsible for the breach and who received the PHI.

iv) Identify what corrective actions BA took or will take to prevent further incidents of a breach.

v) Identify what BA did or will do to mitigate any deleterious effect of the breach.

vi) Identify BA contact information and procedures the CE may use to request additional information if required.

vii) Provide such other information, including a written report, as CE may reasonably request.

i) BA is not an agent of CE.

j) 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.

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:

i) 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.

ii) 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.

k) 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.

l) 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.

m) 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.

n) 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.

o) 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.

Upon agreement execution and prior to any system entering a production state or containing production or protected 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.

p) 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.

q) 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.

r) 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.

s) 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.

t) Minimum Necessary and Limited Data Set: BA's use, disclosure, or request of PHI shall utilize a Limited Data Set (PHI that excludes direct identifiers per 45 CFR §164.514(e)(2)), whenever possible. Otherwise, BA shall, in its performance of the functions, activities, services, and operations, 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.

u) 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).

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.

d) 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.

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

(1) Destruction verification: Complete all such return or provide an attestation of destruction within thirty (30) calendar days after the effective date of the termination, cancellation, expiration, or other conclusion of the contract.

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

ii) 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.

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) 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.

14) Privacy Point of Contact: All communications occurring because of this BAA shall be sent to the CE Privacy Official.

    1) Privacy:

        a) **Covered Entity E-mail**: privacyofficial@alaska.gov

        b) **Business Associate E-mail**: _____

    2) Security:

        a) **Covered Entity E-mail:** doh.its.dso@alaska.gov

        b) **Business Associate E-mail**: _____

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