STATE OF ALASKA
DEPARTMENT OF HEALTH & SOCIAL SERVICES
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA")
BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement is between the State of Alaska, Department of Health and Social Services ("Business Associate" or "BA") and [HOSPITAL] ("Covered Entity" or "CE").

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 created, received, transmitted, or maintained 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;

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" has the same meaning as the term "business associate" at 45 C.F.R. 160.103.

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

3) Designated Record Set: "Designated Record Set" means (i) medical records, billing records, enrollment, payment, claims adjudication, and case or medical management records systems maintained by CE in AKAIMS; or (ii) records used, in whole or in part, by CE to make decisions about individuals. For purposes of this definition, the term "record" means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for CE.

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

2. Permitted Uses and Disclosures by Business Associate.

a. BA may only use or disclose PHI for the following purposes: Tracking utilization, cost and quality of care; analyzing disease burden in state and local populations; analyzing incidence of domestic violence, child abuse and neglect, and admissions related to mental health and substance abuse conditions; research; public health; health care operations.

b. BA may use or disclose PHI as required by law, to carry out the proper management and administration of BA, and to carry out the legal responsibilities of BA.

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

d. 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 in subparagraphs b and e.

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

3. 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 substantially 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 two 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.

c. Reporting Unauthorized Disclosures and Breaches: During the term of this BAA, BA shall notify CE within 15 days 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. 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. 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 make every reasonable effort to correct any deficiencies it caused that result in Breaches of security; intrusion; or unauthorized acquisition, access, use, and disclosure.

   If the unauthorized acquisition, access, use or disclosure of CE's PHI involves only Secured PHI, BA shall notify CE within 30 days of discovering the Breach but is not required to notify CE of the names of the individuals affected.

   If BA discovers a breach of personal information on a state resident, as defined in AS 45.48.090, BA shall immediately after discovering the breach notify CE of the breach and cooperate with CE as necessary to allow CE to comply with the notice requirements of AS 45.48.010. In this paragraph, "cooperate" means sharing with CE information relevant to the breach, except for confidential business information or trade secrets. If CE determines that there is not a reasonable likelihood that harm to consumers whose personal information has been acquired has resulted or will result from the breach, that determination shall be documented in writing and promptly provided to BA.

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.

f. Availability of Information to CE: Upon written statement by CE that it is unable to provide access on its own, and within 30 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 30 days of a written request by CE, BA shall make the accounting record available to CE.

h. Amendment of PHI: Upon written statement by CE that it is unable to provide access on its own, and 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: In the event of a breach caused by BA, BA shall make its internal practices, books and records relating to the use and disclosure of CE's PHI available to the U.S. Department of Health and Human Services to determine CE's and BA's compliance with HIPAA, the HITECH Act and the Privacy and Security Rule.

j. 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.

k. 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.

4. Obligations of CE.

a. CE shall comply with HIPAA, the HITECH Act and the Privacy and Security Rule in maintaining and ensuring the confidentiality, privacy and security of PHI transmitted to BA under the BAA until the PHI is received by BA.

b. CE shall 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.

c. CE shall provide BA with the notice of privacy practices that CE produces in accordance with 45 C.F.R. 164.520, as well as any changes to such notice.

d. CE shall provide BA with any changes in, or revocation of, permission by an individual to use or disclose PHI, if such changes affect BA's permitted or required uses and disclosures.

e. CE shall notify BA of any restriction to the use or disclosure of PHI that CE has agreed to in accordance with 45 C.F.R. 164.522.

5. Termination.

a. Breach: A breach of a material term of the BAA by either party 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 and the Commissioner of the Alaska Department of Health and Social Services.

c. Effect of Termination: Upon termination of the contract for any reason, 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. If destruction or return of PHI is not feasible, BA shall continue to hold the PHI until the PHI provided by CE to BA is either destroyed or returned to CE or six years has passed, whichever is sooner. Upon termination, CE assumes all responsibility for complying with the administration requirements of HIPAA, the HITECH Act, and the Privacy and Security Rule, including, but not limited to, amendment, accounting of disclosures, and notices of privacy practices. BA does not retain any of these responsibilities as to CE's PHI.

6. 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, the parties agree to amend this BAA to ensure compliance with changes in law.

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

8. 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.

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

10. 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 both parties 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.

11. 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.

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

[Name]	Jill Lewis Date
[Title]	Deputy Director
[Hospital]	State of Alaska Department of Health and Social Services Division of Public Health