# Appendix E
# State of Alaska, Department of Health
# HIPAA AND HITECH Information Security Agreement (ISA)

This agreement, effective upon the date of full contract execution, is entered into by and between the **Department of Health** (hereafter known as **Covered Entity**) and _____(hereafter known as **Business Associate**). This agreement is in accordance with **Covered Entity's** 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** and **Business Associate** 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.

**A. Definitions**

1. **"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 **Covered Entity** or **Business Associate**, 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:
   a. Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a **Covered Entity** or **Business Associate**, if access was in good faith and within the scope of authority; or
   b. Inadvertent disclosure by a person authorized to access the PHI to another person authorized to access the PHI.
2. **"Business Associate"** shall mean an individual or entity who or which performs a function or activity on behalf of, or provides a service, to **Covered Entity** 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.
3. **"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. **Covered Entity** 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.
4. "**Data Aggregation**" shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 CFR 164.501.
5. "**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.
6. "**Designated Record Set**" shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 CFR 164.501.
7. **"Electronic Protected Health Information"(**ePHI) shall mean PHI maintained or transmitted in electronic form.

8. **"Health Care Operations"** shall have the meaning as defined under the HIPAA Rules, including, but not limited to, 45 CFR 164.501.
9. **"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).
10. **"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)).
11. **"Minimum Necessary". Business Associate** shall only request, use, and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use, or disclosure.
12. **"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.
13. **"Privacy Official"** shall mean the **Covered Entity's** designated individual, and such individual's designees, who are responsible for the development and implementation of **Covered Entity's** policies and procedures regarding privacy and confidentiality of PHI.
14. **"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.
15. **"Required by law"** shall have the meaning given to such term as stated within 45 CFR 164.103.
16. **"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 **Covered Entity**. (See 45 CFR 164.304).
17. **"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.

**B. Privacy and Security of PHI**

1. **Permitted Uses and Disclosures. Business Associate** is permitted or required to use or disclose PHI it creates, receives, maintains, or transmits in service to **Covered Entity** only as follows:
   a. **Functions and Activities on Covered Entity's Behalf**. **Business Associate** is permitted to use and disclose the minimum necessary PHI it creates, receives, maintains, or transmits to/from **Covered Entity,** 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 **Covered Entity** itself made the use or disclosure.
   b. **Marketing and Fundraising**. Unless expressly authorized by the underlying contract between the parties, **Business Associate** shall not Use or Disclose PHI for any marketing or fundraising purpose.
   c. **Audit**. For purposes of determining **Business Associate's** compliance with HIPAA, upon request of **Covered Entity** or the Secretary of HHS, **Business Associate** shall:
      i. 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 **Covered Entity**.
      ii. Provide reasonable access to **Business Associate's** facilities, equipment, hardware, and software used for the maintenance or processing of **Covered Entity's** PHI.
   d. **Record Keeping**. Business Associate 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 Business Associate's workforce HIPAA education and training, documentation related to any breach, Business Associate Agreements issued to third parties with whom Business Associate discloses PHI for Business Associate's proper management and administration, or as required by law.

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

2. **Prohibition on Unauthorized Use or Disclosure**. **Business Associate** shall neither use nor disclose PHI it creates, receives, maintains, or transmits in service to **Covered Entity**, except as permitted or required by the contract, as required by law, or as otherwise permitted in writing by **Covered Entity**. **Business Associate** acknowledges that **Business Associate** 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.
3. **Offshoring Prohibition. Business Associate** may not transmit, store, process, or make PHI accessible to any recipient outside the United States of America without **Covered Entity's** prior written consent.
4. **Compliance with Laws; Regulatory Amendments. Business Associate** 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.
5. **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 **Business Associate** on behalf of **Covered Entity**.
6. **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.
7. **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.
8. **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.
9. **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.
10. **Information Safeguards**. **Business Associate** 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 **Covered Entity** 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. **Business Associate** 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 **Covered Entity's** request, either orally or in writing, provide **Covered Entity** with a copy of its policies and procedures related to such safeguards. **Business Associate** 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 **Business Associate** in the same manner that such sections apply to **Covered Entity** 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 Entity** shall also apply to **Business Associate** and are incorporated into this Information Security Agreement.

11. **Subcontractors and Agents**. **Business Associate** shall require any of its subcontractors and agents to which **Business Associate** is permitted by this agreement or in writing by **Covered Entity** 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 **Business Associate** 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 **Business Associate** 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 **Business Associate**, and the **Business Associate** shall provide notification to the **Covered Entity,** of any instance of which the agent, subcontractor, or other third party becomes aware in which the confidentiality of such PHI was breached.

12. **Minimum Necessary and Limited Data Set. Business Associate's** use, disclosure, or request of PHI shall utilize a limited data set, whenever possible. Otherwise, **Business Associate** 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 **Business Associate** shall not be obligated to comply with the minimum necessary limitations with respect to those exceptions specified in 45 CFR 164.502 (b)(2). **Business Associate** 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.

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

14. **Risk Assessment.** Upon agreement execution, and prior to any system entering a production state or containing production data, Business Associate must complete **Covered Entity'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 **Covered Entity's** security standards and the **Covered Entity's** selected standards for HIPAA compliance. This security assessment process must be updated and

reassessed 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 updated to reflect the current risk profile of the system.

**C. PHI Access, Amendment, Restriction, and Reporting**

1. **Access.** **Business Associate** shall, upon **Covered Entity'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 **Business Associate** created or received for or from **Covered Entity** and that is in **Business Associate's** custody or control. **Business Associate** shall provide such information in an electronic format, if requested by the individual, and as directed by **Covered Entity**.
2. **Amendment.** **Business Associate** shall, upon receipt of notice from **Covered Entity**, promptly amend or permit **Covered Entity** access to amend, any portion of an individual's PHI which **Business Associate** created or received for or from **Covered Entity** and that is in **Business Associate's** custody or control.
3. **Restriction.** **Business Associate** shall, upon **Covered Entity'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 **Covered Entity's** instructions. **Covered Entity** will promptly notify **Business Associate** in writing of the termination of any such restriction agreement and, with respect to termination of any such restriction agreement, instruct **Business Associate** as to whether any PHI will remain subject to the terms of the restriction agreement.
4. **Reporting.**
   a. Legal or Authorized Disclosure Reporting. Except as permitted by applicable law**,** **Business Associate** 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 **Covered Entity** to comply with relevant statutes and regulations. The report shall be furnished to **Covered Entity** within ten (10) calendar days of its request. In addition, where **Business Associate** is contacted directly by an individual based on information provided to the individual by **Covered Entity**, and where so required by the HITECH Act and/or any accompanying regulations, **Business Associate** shall make such report available directly to the individual.
      i. ***Disclosure Accounting***. Upon request, **Business Associate** shall forward to **Covered Entity** a report of disclosures as required by 45 CFR 164.528, and as applicable, the HITECH Act § 13405(c) and any regulations issued thereunder.
      ii. ***Disclosure Accounting Retention***. **Business Associate** shall maintain an accounting of such disclosures for six (6) years after the date of occurrence.
   b. **Security Incident Reporting**. **Business Associate** shall report to **Covered Entity's** Chief Privacy Officer and Chief Information Security Officer as stipulated in 45 CFR 164.410 after **Business Associate** knows, or should reasonably have known of such Security Incident, any Security Incident of which **Business Associate** becomes aware. In addition, **Business Associate** shall, upon **Covered Entity'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**, Business Associate** shall make a report in accordance with Section C.5, below. If **Business Associate** 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 **Business Associate**, **Business Associate** must take reasonable steps to cure the breach or end the violation and take further actions consistent with 45 CFR 164.504.
   c. **Breach Reporting.** **Business Associate** shall report to **Covered Entity** any breaches of PHI as stipulated in 45 CFR 164.410. **Business Associate** shall make such report to **Covered Entity's** Privacy Officer after **Business Associate** knows, or should reasonably have known, of such breach. **Business Associate** shall cooperate with **Covered Entity** in investigating such breach, and in

meeting **Covered Entity's** obligations under the HITECH Act and any other security breach notification laws. **Business Associate** shall report all breaches to **Covered Entity** in writing (and in the format requested by **Covered Entity**) and such reports shall, at a minimum:

i. Identify the nature of the breach, including the date of the breach and the date of discovery of the breach.

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 **Business Associate** took or will take to prevent further incidents of a breach.

v. Identify what **Business Associate** did or will do to mitigate any deleterious effect of the breach.

vi. Identify **Business Associate** contact information and procedures to enable **Covered Entity** to obtain additional information if required.

vii. Provide such other information, including a written report, as **Covered Entity** may reasonably request.

d. **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)).

5. **Inspection of Books and Records**. **Business Associate** 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, **Covered Entity**) to **Covered Entity** and/or the HHS to determine compliance with the HIPAA Regulations or the **Business Associate's** compliance with this agreement.

6. **Designated Record Set**. **Business Associate** agrees that all PHI received by or created for **Covered Entity** shall be included in an individual's Designated Record Set. **Business Associate** 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.

7. **Restriction Contracts and Confidential Communications.** **Business Associate** shall comply with any agreement that **Covered Entity** 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 **Covered Entity** notifies **Business Associate,** in writing, of the restriction or confidential communication obligations that **Business Associate** must follow. **Covered Entity** will promptly notify **Business Associate** 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 **Business Associate** whether any PHI will remain subject to the terms of the restriction agreement.

**D. Termination and Continuing Privacy and Security Obligations**

1. **Termination of Contract**. As required by the HIPAA Regulations and this agreement**, Covered Entity** may, in addition to other available remedies, terminate the contract if **Business Associate** 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. **Covered Entity** shall exercise this right to terminate the contract by providing **Business Associate** 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 **Covered Entity's** notice of termination. Within thirty (30) calendar days of such termination of the

contract, **Business Associate** shall provide to **Covered Entity** one final report of any and all breaches made of all individuals' PHI during the term of the contract.

2. **Obligations upon Termination.** Upon termination, cancellation, expiration, or other conclusion of the contract, **Business Associate** shall:
   a. As directed by **Covered Entity**, **Business Associate** 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 **Business Associate'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 **Business Associate** created or received for or from **Covered Entity**. Returned PHI must be provided to the **Covered Entity** in a common, nonproprietary, industry standard data format.
   b. 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.
   c. These provisions shall apply to PHI that is in the possession of subcontractors or agents of **Business Associate**.
3. **Continuing Privacy and Security Obligation**. **Business Associate'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 **Covered Entity,** shall be continuous and survive termination, cancellation, expiration, or other conclusion of the contract.
4. **Termination for Cause.** Without limiting the termination rights of the parties pursuant to the contract and upon **Covered Entity's** knowledge of a material breach of this contract by **Business Associate, Covered Entity** shall either:
   a. Provide an opportunity for **Business Associate** to cure the breach or end the violation and, if **Business Associate** does not cure the breach or end the violation within the time specified by **Covered Entity**, terminate the contract, if feasible; or
   b. Immediately terminate the contract if cure is not possible, if feasible.
5. **Effect of Termination.**
   a. Except as provided in paragraph (2) of this Section, upon termination of the contract for any reason, as directed by **Covered Entity**, **Business Associate** shall promptly return or destroy all PHI received from or created or received by **Business Associate** on behalf of, **Covered Entity** that **Business Associate** maintains in any form and retain no copies. This provision shall apply to PHI that is in the possession of subcontractors or agents of **Business Associate**. Returned PHI must be provided to the **Covered Entity** in a common, nonproprietary, industry standard data format.
   b. In the event that **Business Associate** reasonably believes that returning or destroying the PHI is infeasible**, Business Associate** shall provide to **Covered Entity** prompt notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return, or destruction is infeasible, **Business Associate** 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 **Business Associate** maintains such PHI.

**E. 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.

**F. 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: _____

**Submission Instructions:**

**Business Associate:** Please return the signed form with your submission.

**DOH Recipient:** Please submit the signed form to the HelpDesk and state ***'Please direct to the CTO'*** in the ticket and include the **Contractor Business Name** and **DOH Project Name** as well.