| TITLE: HIE System Security | |
|---|---|
| Policy #: HEN-013 | Effective Date: April 4, 2012 |
| Program: Hawai'i HIE | Revision Date: November 16, 2016 |
| Approved By: Hawai'i HIE Board of Directors | |

**Table of Contents**

## 1. Purpose

This document identifies the security safeguards pertaining to the Hawai'i HIE's Health eNet system ("Health eNet", the "System") that shall be implemented by the Hawai'i HIE and Health eNet Participants. The document provides references to other Hawai'i HIE Operational Policies and Procedures that specifically address the details of a number of these safeguards.

## 2. Scope

This policy applies to: 1) the Hawai'i HIE and all of its workforce members, 2) all Health eNet Authorized Users, 3) all Hawai'i HIE business associates, subcontractors, and 4) all Health eNet Participants.

## 3. Definitions

A number of terms and phrases utilized in this Operational Policies and Procedures document are defined in the HEN-000, *Definitions* document, as well as in the various Operational Policies and Procedures referenced in this document.

## 4. Policy

The Hawaii HIE's Operational Policies and Procedures define the administrative requirements; process steps to implement reasonable physical and technical safeguards involved in managing the security of the Hawai'i HIE Health eNet System; and the required documentation involved in safeguarding the data, including electronic protected health information (ePHI), contributed to, managed by and exchanged via the System.

**4.1. Administrative Safeguards.** The Hawai'i HIE and Health eNet Participants shall adopt administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of their respective workforce members in relation to the protection of that information.

**4.1.1. Security Management and Evaluation Process.** The Hawai'i HIE and each Participant that is a HIPAA covered entity shall implement policies and procedures to implement its information security program for preventing, detecting, containing and correcting security violations under their respective policies and procedures, and applicable laws; evaluate; and as necessary amend elements to its security program.

| **Procedure** |
| --- |
| 1. Please refer to the Hawai'i HIE *Security Management and Evaluation Process* Policy and Procedure. |

**4.1.2. Sanctions.** The Hawai'i HIE shall apply appropriate sanctions, e.g. disciplinary actions, against workforce members who fail to comply with the Hawai'i HIE Operational Policies and Procedures, or otherwise violate HIPAA, or other federal or state law safeguarding personally identifiable information. For workforce

members of Participants responsible for such violations, the Hawai'i HIE will defer to the policies and procedures of the Participants.

| **Procedure** |
|---|
| 1. Please refer to the Hawai'i HIE *Sanctions* policy and procedure, and the Hawai'i HIE HEN-005 *Access Management* Operational Policy and Procedures. |

**4.1.3. Assigned Security and Privacy Responsibilities.** The Hawai'i HIE and each Participant shall identify their respective "security official" (i.e. Security Officer) and "privacy official" (i.e. Privacy Officer) who are responsible for the development and implementation of the policies and procedures required by HIPAA and other applicable laws pertaining to privacy and security of individually identifiable health information.

| **Procedure** |
|---|
| 1. As required in the Hawai'i HIE HEN-003 *Participating Entity Registration and Compliance Requirements* Operational Policy and Procedures, the Hawai'i HIE and all Participants shall each designate a Security Officer and Privacy Officer. One workforce member for each entity may fulfill both roles for his/her entity. |

**4.1.4. Workforce Security.** The Hawai'i HIE and each Participant that is a HIPAA covered entity shall implement policies and procedures to identify their respective workforce members who need access to electronic protected health information (ePHI), provide such authorized workforce members with the appropriate access to ePHI, and prevent those workforce members who do not have authorized access from obtaining access to ePHI.

| **Procedures** |
|---|
| 1. **Authorization and/or Supervision.** Please refer to the Hawai'i HIE HEN-005 *Access Management*, HEN-010 *HIE System Audit*, HEN-012 *Incident Response and Mitigation* Operational Policies and Procedures. |
| 2. **Workforce Clearance Procedure.** Please refer to the Hawai'i HIE HEN-005 *Access Management* Operational Policy and Procedures.<br><br>Participants shall adhere to their respective policies and procedures regarding workforce background checks and other workforce-related verification protocols. |
| 3. **Termination Procedure.** Please refer to the Hawai'i HIE HEN-005 *Access Management*, HEN-010 *HIE System Audit*, HEN-012 *Incident Response and Mitigation* policies and procedures. |

**4.1.5. Information Access Management.** The Hawai'i HIE and each Participant that is a HIPAA covered entity shall implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of 45 CFR 164 Subpart E (i.e. HIPAA Privacy Rule).

| Procedures |
|---|
| 1. **Access Authorization.** Implement policies and procedures for granting access to ePHI via the Health eNet. Please refer to Hawai'i HIE HEN-003 *Participating Entity Registration and Compliance Requirements* and HEN-005 *Access Management* Operational Policies and Procedures. |
| 2. **Access Establishment and Modification.** Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify access to the Health eNet. Please refer to HEN-004 *Participation Suspension, Termination and Reinstatement*, HEN-005 *Access Management*, and HEN-010 *HIE System Audit* Operational Policies and Procedures. |

**4.1.6. Security Awareness and Training.** The Hawai'i HIE shall implement a security awareness and training program for all members of their respective workforce members, including management.

#### 4.1.6.1. Hawai'i HIE Workforce Training

| Procedures |
|---|
| 1. **Hawai'i HIE New and Returning Workforce Members.** Hawai'i HIE compliance officers shall provide training to a workforce member hired for the first time by the Hawai'i HIE, and to any returning workforce member who last received Hawai'i HIE security awareness training more than one (1) year prior to his/her current work start dates, within one (1) month of the workforce member's current work start date. |
| 2. **Hawai'i HIE Ongoing Training.** Hawai'i HIE compliance officers shall provide training to each Hawai'i HIE workforce member at least once per year. Ongoing training shall include security updates and reminders, e.g. in the event of changes to Hawai'i HIE policies and procedures related to security of PHI. |

#### 4.1.6.2. Participant Workforce Training

| Procedure |
|---|
| 1. Participants shall follow their respective policies and procedures for providing security awareness and training to their workforce members. |

**4.1.7. Security Incident Procedures.** The Hawai'i HIE, in cooperation with Participants as necessary, shall identify and respond to suspected or known Security Incidents; mitigate, to the extent practicable, harmful effects of Security Incidents that are known to the Hawai'i HIE; and document Security Incidents and their outcomes.

| Procedure |
|---|
| 1. **Incident Response and Reporting.** Please refer to the Hawai'i HIE HEN-012 |

| |
|---|
| *Incident Response and Mitigation* Operational Policy and Procedure. |

**4.1.8. Contingency Plan.** The Hawai'i HIE and each Participant that is a HIPAA covered entity shall establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

| **Procedure** |
|---|
| 1. Please refer to the Hawai'i HIE HEN-005 *Access Management* Operational Policy and Procedures, and the Hawai'i HIE Contingency Plan policy and procedures. |

**4.1.9. Business Associate Agreements**

**4.1.9.1. BAAs Between Covered Entity Participants and the Hawai'i HIE.** The Hawai'i HIE shall enter into a contract, as specified in 45 CFR 164.314 and 45 CFR 164.504, with each Participant that is a HIPAA covered entity.

| **Procedures** |
|---|
| 1. Each HIPAA covered entity Participant shall execute a Business Associate Agreement (BAA) with the Hawai'i HIE, as provided for in the Hawai'i HIE HEN-003 *Participating Entity Registration and Compliance Requirements* Operational Policy and Procedures.<br><br>Each HIPAA covered entity Participant may utilize its BAA template, or utilize Exhibit B, "Sample Subcontractor Business Associate Agreement" as a template, for BAAs with the Hawai'i HIE.<br><br>The Hawai'i HIE Executive Director shall be the signatory for the Hawai'i HIE. |
| 2. The Hawai'i HIE shall retain a copy of each executed BAA for a minimum of six (6) years from the date of termination, or last in effect, whichever is later. |

**4.1.9.2. Hawai'i HIE Subcontractor BAAs.** The Hawai'i HIE shall enter into contracts, as specified in 45 CFR 164.314 and 45 CFR 164.504, with vendors, and other persons and entities with which it has a business relationship, that create, receive, maintain, or transmit PHI on behalf of the Hawai'i HIE, i.e. "subcontractors", as defined in 45 CFR 160.103.

| **Procedures** |
|---|
| 1. The Hawai'i HIE shall, on an ongoing basis, identify its subcontractors, including those with which the Hawai'i HIE has or will have a temporary, or otherwise finite business relationship. |

| |
|---|
| 2. The Hawai‘i HIE and each identified subcontractor shall execute a subcontractor BAA.<br><br>The Hawai‘i HIE may utilize Exhibit B, “Sample Subcontractor Business Associate Agreement”, as a template for BAAs with its subcontractors.<br><br>The Hawai‘i HIE Executive Director, or a member of the Hawai‘i HIE management team designated by the Executive Director, shall be the signatory for the Hawai‘i HIE. |
| 3. The Hawai‘i HIE shall, in cooperation with its subcontractors, periodically amend subcontractor BAAs as necessary to address updates to regulations and regulatory guidance pertaining to BAAs, and/or changes to the business arrangement between the Hawai‘i HIE and a given subcontractor. |
| 4. The Hawai‘i HIE shall retain a copy of each executed subcontractor agreement for a minimum of six (6) years from the date of termination, or last in effect, whichever is later. |

**4.2. Physical Safeguards.** The Hawai‘i HIE shall implement physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

**4.2.1. Facility Access Controls.** The Hawai‘i HIE shall implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

| **Procedure** |
|---|
| 1. Please see the Hawai‘i HIE *Facility Access Controls* policy and procedure. |

**4.2.2. Workstation, Device and Media Safeguards.** The Hawai‘i HIE shall implement policies and procedures that address appropriate use of and safeguards for computing workstations, laptops and other transportable devices, and transportable electronic media.

| **Procedure** |
|---|
| 1. Please see the Hawai‘i HIE *Workstation, Device and Media Safeguards* policy and procedure. |

**4.3. Technical Safeguards.** The Hawai‘i HIE and Health eNet Participants shall adopt technology and policies and procedures for its use that protect ePHI and control access to it.

**4.3.1. Access Controls.** The Hawai‘i HIE and each Participant shall implement technical policies and procedures for electronic information systems that maintain ePHI to

allow access only to those persons or software programs that have been granted access rights.

| Procedure |
| --- |
| 1. Please refer to the Hawai‘i HIE HEN-005 *Access Management* Operational Policy and Procedures. |

**4.3.2. Audit Controls and System Activity Review.** The Hawai‘i HIE and each Participant shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

| Procedure |
| --- |
| 1. Please refer to the Hawai‘i HIE HEN-010 *HIE System Audit* Operational Policy and Procedures. |

**4.3.3. Integrity.** The Hawai‘i HIE and each Participant shall implement policies and procedures to protect ePHI from improper alteration or destruction.

| Procedure |
| --- |
| 1. Please refer to the Hawai‘i HIE HEN-011 *Data Integrity* Operational Policy and Procedures. |

**4.3.4. Person and Entity Authentication and Verification.** The Hawai‘i HIE and each Participant shall implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

**4.3.4.1. Authentication and Verification of Health eNet Authorized Users**

| Procedure |
| --- |
| 1. Please refer to the Hawai‘i HIE HEN-003 *Participating Entity Registration and Compliance Requirements* and HEN-005 *Access Management* Operational Policies and Procedures. |

**4.3.4.2. Authentication and Verification of Individuals Seeking Access to ePHI**

| Procedure |
| --- |
| 1. Please refer to the HEN-008 *Individual Notice Participation* and HEN-009 *Individual Rights* Operational Policy and Procedures. |

**4.3.5. Transmission Security.** The Hawai‘i HIE shall implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

| Procedure |
| --- |
| 1. Please refer to the Hawai‘i HIE HEN-005 *Access Management* and HEN-011 *Data Integrity* Operational Policies and Procedures. |

**4.4. Documentation Requirements.** The Hawai'i HIE, in cooperation with Participants and other stakeholders as necessary, shall address the requirements regarding implementation, maintenance and retention of policies, procedures and other documentation set forth in HIPAA (45 CFR 164.316 and 45 CFR 164.530) applicable to the Hawai'i HIE as a business associate, and as set forth in other applicable laws.

**4.4.1. Policies and Procedures.** The Hawai'i HIE shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of HIPAA, and as set forth in other applicable laws.

| **Procedure** |
|---|
| 1. **Health eNet Operational Policies.** Please see the Hawai'i HIE HEN-001 *Governing Principles* and HEN-002 *Policy Development and Approval Process* Operational Policies and Procedures. |

**4.4.2. Documentation.** The Hawai'i HIE shall maintain the policies and procedures implemented to comply with HIPAA and other applicable laws in written (which may be electronic) form; and if an action, activity or assessment is required by law and/or the Hawai'i HIE's policies and procedures to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

| **Procedure** |
|---|
| 1. Please see the Hawai'i HIE *Documentation* policy and procedure. |

## 5. Revision History

| Revision Date | Revision Type* | Author(s) | Revision Rationale, Description | Approved by |
|---|---|---|---|---|
| April 4, 2012 | New | Legal/Policy Committee (policy sub-committee) | Initial version of policy | Hawai'i HIE Board of Directors |
| Nov 16, 2016 | Amendment | Legal/Policy Committee | Table of contents, section numbering and procedures added; existing definitions and policy sections edited to reflect current Health eNet services and operations | Hawai'i HIE Board of Directors |

* Revision Type options = New, Amendment, Minor Amendment, Consolidation (i.e. merging of multiple policies)

## Exhibit A. Sample Business Associate Agreement
## BUSINESS ASSOCIATE AGREEMENT

(If Participant is a HIPAA covered entity, Participant's BAA may be used for this exhibit)

This Business Associate Agreement ("BAA") "is entered into by and between Hawai'i Health Information Exchange (HIE) ("Business Associate") and the Participant ("Covered Entity") named in the Parties' Data Sharing Agreement ("Agreement"), effective as of the Effective Date of the Agreement. This BAA is incorporated by reference into the Agreement and does not require signatures of the Parties on this Exhibit to be fully enforceable.

WHEREAS, Covered Entity and Business Associate are entering into a Data Sharing Agreement contemporaneously with this BAA; and

WHEREAS, pursuant to the Administrative Simplification provisions of HIPAA, HHS promulgated the Privacy Standards at 45 C.F.R. Parts 160 and 164, requiring Covered Entities to protect the privacy of PHI; and

WHEREAS, pursuant to HIPAA, HHS has issued the Security Standards at 45 C.F.R. Parts 160, 162 and 164, for the protection of Protected Health Information including electronic Protected Health Information ("PHI"); and

WHEREAS, in order to protect the privacy and security of PHI, created or maintained by or on behalf of the Covered Entity, the Privacy Standards and Security Standards require a Covered Entity to enter into a "business associate agreement" with certain individuals and entities providing services for or on behalf of the Covered Entity if such services require the use or disclosure of PHI or ePHI; and

WHEREAS, on February 17, 2009, the HITECH Act was signed into law. The HITECH Act imposes certain additional privacy and security obligations on Covered Entities; and

WHEREAS, the HITECH Act extended certain HIPAA and HITECH Act requirements directly to business associates; and

WHEREAS, the HITECH Act requires that certain of its provisions be included in business associate agreements, and that certain requirements of the Privacy Standards be imposed contractually upon Covered Entities as well as business associates; and

WHEREAS, Business Associate and Covered Entity desire to enter into this Business Associate Agreement to achieve the goals and purposes of the Agreement;

NOW THEREFORE, in consideration of the mutual promises set forth in this BAA and the Data Sharing Agreement, and other good and valuable consideration, the sufficiency and receipt of which are hereby severally acknowledged, the parties agree as follows:

1. Definitions. Terms defined in the Agreement retain their same meaning in this BAA and definitions in this BAA are incorporated by reference into the Agreement, except as provided in this Section. All capitalized terms not otherwise defined in this BAA shall have the meanings set forth in the Privacy Standards, Security Standards or the HITECH Act, as applicable (collectively referred to hereinafter

as the “Confidentiality Requirements”).

a. "Security Incident" is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system. 45 CFR § 164.304.
b. For purposes of this BAA only, all references to "PHI" in this BAA shall be limited to PHI received by Business Associate from Covered Entity or created or received by Business Associate on behalf of Covered Entity.

2. Covered Entity Obligations. Covered Entity shall not knowingly submit records to Business Associate that contain Restricted Information or other information not permitted within the HIE System (“Restricted Information”), as described in the Agreement. Covered Entity shall notify Business Associate within five (5) working days from the date it becomes aware of Restricted Information submitted by Covered Entity.

3. Business Associate Obligations. Business Associate may receive from Covered Entity, or create or receive on behalf of Covered Entity, health information that is protected under applicable state and/or federal law, including without limitation, PHI. Business Associate agrees not to use or disclose (or permit the use or disclosure of) PHI in a manner that would violate the Confidentiality Requirements if the PHI were used or disclosed by Covered Entity in the same manner. Business Associate shall:
    a. comply with HIPAA, the HITECH Act, and all applicable Regulations;
    b. use PHI in compliance with 45 C.F.R. § 164.504(e), except as otherwise required by law;
    c. not use or further disclose the information it obtains under the Agreement other than as permitted or required by the Agreement or as required by law;
    d. use appropriate safeguards and comply, where applicable, with 45 C.F.R. Subpart C to prevent use or disclosure of the information other than as provided by the Agreement; and
    e. report to the Covered Entity within five (5) days of Business Associate becoming aware of any use or disclosure of the information not permitted in the Agreement or this BAA, including breaches of unsecured PHI as required by 45 C.F.R. § 164.410.

4. Disclosure of PHI. Subject to any limitations in this BAA, Business Associate may disclose PHI to any third party persons or entities (“Subcontractors”) as necessary to perform its obligations under the Agreement and as permitted or required by applicable federal or state law. Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees to:
    a. the same restrictions and conditions that apply to Business Associate with respect to such information; and
    b. comply with applicable requirements of 45 C.F.R. Subpart C, including implementation of reasonable and appropriate safeguards to protect electronic PHI, by entering into a contract or other arrangement that complies with 45 C.F.R. § 164.314.

5. Duty to Mitigate. Business Associate agrees to mitigate, to the extent practical and unless otherwise requested by Covered Entity in writing, any harmful effect that is known to Business Associate and is the result of a use or disclosure of PHI by Business Associate (or any of Business Associate's Authorized Users, agents or contractors) in violation of the Agreement or this BAA.

6. Individual Rights Regarding Designated Record Sets. Business Associate shall:
    a. provide access to, and permit inspection and copying of, PHI by Covered Entity or, as

directed by Covered Entity, an individual who is the subject of the PHI under conditions and limitations required under 45 CFR § 164.524, as it may be amended from time to time;

b. notify Covered Entity within five (5) business days of receipt of any request for access or amendment by an individual. Covered Entity shall determine whether to grant or deny any access or amendment requested by the individual;
c. make PHI that is part of the individual's designated record set maintained by Covered Entity available for amendment by Covered Entity, and incorporate any amendments to PHI in the HIE System Record Locator Services (RLS) upon the Hawai'i HIE granting an individual's request to amend PHI in the RLS, in accordance with 45 CFR § 164.526, as it may be amended from time to time;
d. provide any information requested under this Section in the form or format (e.g. electronic or hard copy) requested to the Covered Entity or individual who is the subject of the PHI, if it is readily producible in such form or format, to the extent required by HIPAA; and
e. be entitled to charge a reasonable fee based upon its labor costs in responding to a request for electronic information (or a cost-based fee for the production of non-electronic media copies).

7. Accounting of Disclosures. Business Associate shall make available to Covered Entity in response to a request from an individual, information required for an accounting of disclosures of PHI for a period of up to six (6) years with respect to the individual in accordance with 45 CFR § 164.528 and any related regulations or guidance issued by HHS in accordance with such provision. Business Associate shall provide to Covered Entity such information necessary to provide an accounting pursuant to Covered Entity's request within the time required by state or federal law. Such accounting must be provided without cost to the individual or to Covered Entity within a twelve (12) month period per accounting request. For subsequent accountings within a twelve (12) month period, Business Associate may charge a reasonable fee based upon the Business Associate's labor costs in responding to a request for electronic information (or a cost-based fee for the production of non- electronic media copies) so long as Business Associate informs the Covered Entity and the Covered Entity informs the individual in advance of the fee, and the individual is afforded an opportunity to withdraw or modify the request. Such accounting obligations shall survive termination of this BAA and shall continue as long as Business Associate maintains PHI.

8. Withdrawal of Authorization. Business Associate agrees to cease the use and disclosure of an individual's PHI provided that:
    a. The Business Associate's use or disclosure is based upon the patient's authorization for the use of the patient's PHI; and
    b. Business Associate has notice from the Covered Entity or patient that:
        i. the individual patient revokes such authorization in writing,
        ii. the effective date of such authorization has expired,
        iii. the condition set forth in the authorization is no longer in effect or has expired, or
        iv. the consent or authorization is found to be enforced in any manner that renders it invalid.

    Nothing in this Section is intended to require Business Associate to cease the use or disclosure of PHI if Business Associate has relied on such use or disclosure, where an exception under the Confidentiality Requirements expressly applies, or until clarification from the individual is received by Business Associate if reasonably requested.

9. Records and Audit. Business Associate shall make available to the HHS Secretary or its agents, its

internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received by Business Associate on behalf of Covered Entity for the purpose of determining Covered Entity's compliance with the Confidentiality Requirements or any other health oversight agency, in a time and manner designated by the Secretary. Except to the extent prohibited by law, Business Associate agrees to notify Covered Entity within five (5) business days of its receipt of any and all requests by or on behalf of any and all federal, state and local government authorities served upon Business Associate for PHI.

10. Indemnification. Indemnification shall be as set forth in the General Terms and Conditions of the Agreement.

11. Compliance with the Security Rule. To the extent that Business Associate creates, receives, maintains, or transmits ePHI, Business Associate shall also implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any ePHI that Business Associate may create, receive, maintain or transmit on behalf of Covered Entity in conformity with the requirements of the Security Rule as amended by the HITECH Act. Business Associate shall also implement policies and procedures and comply with documentation requirements in compliance with the Security Rule as amended by the HITECH Act.

12. Implementation of Security Standards Notice of Security Incidents. Business Associate acknowledges that the HITECH Act requires Business Associate to comply with 45 C.F.R. § 164.308, 164.310, 164.312 and 164.316 as if Business Associate were a Covered Entity and Business Associate agrees to comply with these provisions of the Security Standards and all additional security provisions of the HITECH Act. Furthermore, to the extent feasible, Business Associate will use commercially reasonable efforts to ensure that the technology safeguards used by Business Associate to secure PHI will render such PHI unusable, unreadable and indecipherable to individuals unauthorized to acquire or otherwise have access to such PHI in accordance with HHS Guidance published at 74 Federal Register 19006 (April 17, 2009), or such later regulations or guidance promulgated by HHS or issued by the National Institute for Standards and Technology ("NIST") concerning the protection of identifiable data such as PHI. Business Associate shall report to Covered Entity any Successful Security Incident of which it becomes aware within five (5) business days. At a minimum, such report shall contain the following information to the degree that the information is known at the time of reporting:
    (i.) date and time when the Security Incident occurred and/or was discovered;
    (ii.) names of systems, programs, or networks affected by the Security Incident;
    (iii) preliminary impact analysis;
    (iv) description of and scope of ePHI used, disclosed, modified, or destroyed by the Security Incident; and
    (v) provide a report of any mitigation steps taken.

    Any Security Incident that is a Breach of Unsecured PHI shall be reported pursuant to Section 13.

13. Reporting of Privacy Incidents.
    13.1 Breach Notification to Covered Entity and Mitigation. Business Associate agrees to implement reasonable systems for the discovery and prompt reporting to Covered Entity of any "breach" of "unsecured PHI" as those terms are defined by 45 C.F.R. §164.402 or upon notice or any reasonable belief that a "breach" has occurred (hereinafter a "HIPAA Breach"). The Parties acknowledge and agree that 45 C.F.R. §164.404, as described below in this Section, governs the determination of the date of a Breach. In the event of any

conflict between this Section and the Confidentiality Requirements, the more stringent requirements shall govern. Business Associate will, following the discovery of a Breach, notify Covered Entity immediately and in no event later than the first day (24 hrs) after Business Associate discovers such Breach, unless Business Associate is prevented from doing so by 45 C.F.R. §164.412 concerning law enforcement investigations. For purposes of reporting a Breach to Covered Entity, the discovery of a Breach shall occur as of the first day on which such Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. Business Associate will be considered to have had knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the Breach) who is an employee, officer or other agent of the Business Associate. No later than seven (7) business days following a Breach, Business Associate shall provide Covered Entity with sufficient information to permit Covered Entity to comply with the Breach notification requirements set forth at 45 C.F.R. § 164.400 et seq. Specifically, if the following information is known to (or can be reasonably obtained by) the Business Associate, Business Associate will provide Covered Entity with:

(i) contact information for individuals who were or who may have been impacted by the Breach (e.g., first and last name, mailing address, street address, phone number, email address);

(ii) a brief description of the circumstances of the Breach, including the date of the Breach and date of discovery;

(iii) a description of the types of unsecured PHI involved in the Breach (e.g., names, social security number, date of birth, address(es), account numbers of any type, diagnostic and/or billing codes and similar information);

(iv) a brief description of what the Business Associate has done or is doing to investigate the Breach, mitigate harm to the individual impacted by the Breach, and protect against future Breaches; and

(v) appoint a liaison and provide contact information for same so that the Covered Entity may ask questions or learn additional information concerning the Breach.

Following a Breach, Business Associate will have a continuing duty to cooperate with Covered Entity regarding breach notification and inform Covered Entity of new information learned by Business Associate regarding the Breach, including but not limited to the information described in items (i) through (v), above.

13.2 Data Breach Notification and Mitigation under Other Laws. Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach by Business Associate (or its Recipients) of individually identifiable information (including but not limited to PHI, and referred to hereinafter as "Individually Identifiable Information") that, if misused, disclosed, lost or stolen, Covered Entity believes would trigger an obligation under one or more State data breach notification laws (each a "State Breach") to notify the individuals who are the subject of the information. Business Associate agrees that in the event any Individually Identifiable Information is lost, stolen, used or disclosed by Business Associate (or its Recipients) in violation of one or more State data breach notification laws, Business Associate shall promptly:

(i) cooperate and assist Covered Entity with any investigation into any State Breach or alleged State Breach;

(ii) cooperate and assist Covered Entity with any investigation into any State Breach or

alleged State Breach conducted by HHS or any State Attorney General or State Consumer Affairs Department (or their respective agents) ;

(iii) comply with Covered Entity's reasonable determinations regarding Covered Entity's and Business Associate's obligations to mitigate to the extent practicable any potential harm to the individuals impacted by the State Breach; and

(iv) assist with the implementation of any decision by Covered Entity or any State or Federal agency, including, if necessary, HHS or any State Attorney General or State Consumer Affairs Department (or their respective agents), to notify individuals impacted or potentially impacted by a State Breach.

13.3 Cooperation of Business Associate and Authority of Covered Entity. Business Associate will fully cooperate with Covered Entity in any risk assessment conducted by Covered Entity in order to determine whether any Breach compromises the security or privacy of the PHI. Business Associate will accept Covered Entity's final determination as to whether the PHI was compromised in any situation reported by Business Associate to Covered Entity.

14. Term and Termination.

14.1 This BAA shall commence on the Effective Date of the Agreement and shall remain in effect until terminated in accordance with the terms of this section, provided, however, that termination shall not affect the respective obligations or rights of the parties arising under this BAA prior to the effective date of termination, all of which shall continue in accordance with their terms.

14.2 Covered Entity shall have the right to terminate this BAA for any reason, including determination that Business Associate has violated a material term of the BAA, upon thirty (30) days written notice to Business Associate. Such termination of the BAA shall simultaneously terminate the Agreement on the same effective date, unless otherwise agreed to in writing by both parties.

14.3 In the event that both parties cannot resolve their differences, either Party may immediately terminate this BAA (the "Terminating Party") and shall have no further obligations to the other Party (the "Terminated Party") hereunder, except as provided in Section 14.6 below, if any of the following events shall have occurred and be continuing:

(i.) The Terminated Party fails to observe or perform any material covenant or obligation contained in this BAA for ten (10) days after written notice thereof has been given to the Terminated Party; or

(ii) A violation by the Terminated Party of any provision of the Confidentiality Requirements or other applicable federal or state privacy law relating to the obligations of the Terminated Party under this BAA.

14.4 Termination of this BAA for any of the reasons set forth in Section 5.1 of the Agreement shall be cause for Covered Entity to immediately terminate for cause the Agreement pursuant to which Business Associate is entitled to receive PHI from Covered Entity.

14.5 Upon the termination of the Agreement, this BAA will automatically terminate.

14.6 Upon termination of this BAA for any reason, Business Associate agrees either to return to Covered Entity or to destroy all PHI received from Covered Entity or otherwise through the performance of services for Covered Entity, that is in the possession or control of Business Associate or its agents, unless return or destruction is not feasible or lawful in light of the purposes of the HIE System, or unless other legal grounds exist for retaining the PHI. In the case of PHI which is not returned or destroyed, Business Associate shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, or as otherwise permitted by law, for so long as Business Associate maintains such PHI. Business Associate further agrees to comply with other applicable state or federal law, which may require a specific period of retention, redaction, or other treatment of such PHI.

15. Ineligible Persons. Business Associate represents and warrants to Covered Entity that Business Associate (i) is not currently excluded, debarred, or otherwise ineligible to participate in any federal health care program as defined in 42 U.S.C. § 1320a-7b(f) ("the Federal Healthcare Programs"); (ii) has not been convicted of a criminal offense related to the provision of health care items or services and not yet been excluded, debarred, or otherwise declared ineligible to participate in the Federal Healthcare Programs, and (iii) is not under investigation or otherwise aware of any circumstances which may result in Business Associate being excluded from participation in the Federal Healthcare Programs. This shall be an ongoing representation and warranty during the term of this BAA, and Business Associate shall immediately notify Covered Entity of any change in the status of the representations and warranty set forth in this section. Any breach of this section shall give Covered Entity the right to terminate this BAA immediately for cause.

16. Miscellaneous.

16.1 Notices. All notices, requests, demands and other communications required or permitted to be given or made under this BAA shall be in writing, shall be deemed to have been duly given if transmitted by email or delivered by facsimile, courier service, or personal delivery to the addresses or email addresses listed below, in each case with verification or acknowledgement of delivery, or three (3) days after mailing first class, postage prepaid, return receipt requested, to such address. Hawai'i HIE and Participant may change their own address or email address for purposes of this section by giving the other written notice of the new address or email address.

| If to Business Associate, to: | If to Covered Entity, to: |
|---|---|
| 900 Fort Street Mall, Suite 1305<br>Honolulu, Hawai'i 96813 | _____<br>_____ |
| Attention: Christine Sakuda | Attention: _____ |
| E-mail: csakuda@hawaiihie.org | Email: _____ |

16.2 Waiver. No provision of this BAA or any breach thereof shall be deemed waived unless such waiver is in writing and signed by the Party claimed to have waived such provision or breach. No waiver of a breach shall constitute a waiver of or excuse any different or subsequent breach.

16.3 Assignment. Neither Party may assign (whether by operation or law or otherwise) any of

its rights or delegate or subcontract any of its obligations under this BAA without the prior written consent of the other Party. Notwithstanding the foregoing, Covered Entity shall have the right to assign its rights and obligations hereunder to any entity that is an affiliate or successor of Covered Entity, without the prior approval of Business Associate.

16.4 Severability. Any provision of this BAA that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this BAA or affecting the validity or enforceability of such remaining provisions unless such severance makes the remaining provisions of this BAA impractical to perform, in which case the BAA is terminated.

16.5 Governing Law. This BAA shall be governed by and interpreted in accordance with the laws of the State of Hawai'i, excluding its conflicts of law's provisions, except insofar as governed by federal law (such as HIPAA).

16.6 Equitable Relief. Notwithstanding the Parties' duty to arbitrate all other claims, the Parties understand and acknowledge that any disclosure or misappropriation of any PHI in violation of HIPAA or in violation of this BAA may cause the other Party irreparable harm, the amount of which may be difficult to ascertain, and therefore agrees that any Party shall have the right to apply to a court of competent jurisdiction in Hawai'i for specific performance and/or an order restraining and enjoining any such further disclosure or breach and for such other emergency relief as the Party may deem appropriate, reserving all other claims for binding arbitration. Such rights are to be in addition to the remedies otherwise available at law or in equity. The Parties expressly waive the defense that a remedy in damages will be adequate and further waive any requirement in an action for specific performance or injunction for the posting of a bond.

16.7 Nature of Agreement; Independent Contractor. Nothing in this BAA shall be construed to create (i) a partnership, joint venture or other joint business relationship between the parties or any of their affiliates, or (ii) a relationship of employer and employee between the parties. Business Associate is an independent contractor, and not an agent of Covered Entity. This BAA does not express or imply any commitment to purchase or sell goods or services.

16.8 Interpretation, Changes in Law. Any ambiguity in this BAA shall be resolved to permit the Parties to comply with HIPAA and the HITECH Act.

## Exhibit B: Sample Subcontractor Business Associate Agreement
## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is entered into by and between Hawai'i Health Information Exchange ("Hawai'i HIE") and _____ ("Subcontractor"), effective as of the execution by signature of this BAA.

WHEREAS, pursuant to the Administrative Simplification provisions of HIPAA, the U.S. Department of Health and Human Services (HHS) promulgated the Privacy Standards at 45 CFR Parts 160 and 164, requiring covered entities and business associates to protect the privacy of PHI; and

WHEREAS, pursuant to HIPAA, HHS has issued the Security Standards at 45 CFR Parts 160, 162 and 164, for the safeguarding of Protected Health Information including electronic Protected Health Information ("PHI"); and

WHEREAS, in order to protect the privacy and security of PHI, created, received or maintained by Hawai'i HIE on behalf of covered entities for which Hawai'i HIE is a business associate, the Privacy Standards and Security Standards require a business associate to enter into a "business associate agreement" with certain individuals and entities in the roles of subcontractors providing services for or on behalf of the business associate if such services require the use or disclosure of PHI or ePHI; and

WHEREAS, on February 17, 2009, the HITECH Act was signed into law, and on March 26, 2013, the HIPAA Omnibus Final Rule went into effect. The HITECH Act and Omnibus Final Rule impose certain additional privacy, security, breach notification and enforcement obligations on covered entities, business associates and subcontractors; and

WHEREAS, the HITECH Act and Omnibus Final Rule extended certain HIPAA requirements directly to business associates and subcontractors; and

WHEREAS, the HITECH Act and Omnibus Final Rule requires that certain of their provisions be included in business associate agreements, and that certain requirements of the Privacy Standards be imposed contractually upon covered entities as well as business associates and subcontractors; and

WHEREAS, the Hawai'i HIE and Subcontractor wish to enter into or have entered into various oral and/or written agreements ("Substantive Agreements") whereby Subcontractor will provide certain services to, for, or on behalf of Hawai'i HIE involving the use or disclosure of PHI as defined in the HIPAA Rules (as defined below), and pursuant to such Substantive Agreements, Subcontractor may be considered a "Subcontractor" of Hawai'i HIE as defined below; and

WHEREAS, Hawai'i HIE and Subcontractor desire to enter into this BAA to achieve the goals and purposes of the Substantive Agreements (as defined below);

NOW THEREFORE, in consideration of the mutual promises set forth in this BAA, the Customer Agreement between Hawai'i HIE and Subcontractor, and other good and valuable consideration, the sufficiency and receipt of which are hereby severally acknowledged, the parties agree as follows:

17. Definitions. All capitalized terms not otherwise defined in this BAA shall have the meanings set forth

in the Privacy Standards, Security Standards and other HIPAA Standards, as applicable (collectively referred to hereinafter as the "Confidentiality Requirements").

a. Catch-all definition:
   The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.
b. Specific definitions:
   i. Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean Hawai'i HIE.
   ii. Covered Entity. "Covered entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103.
   iii. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
   iv. Security Incident. "Security Incident" is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system. 45 CFR 164.304.
   v. Subcontractor. "Subcontractor" is a person or entity that creates, receives, maintains or transmits PHI on behalf of a business associate. 45 CFR 160.103.

18. Hawai'i HIE Obligations.
    a. Hawai'i HIE shall notify Subcontractor of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Subcontractor's use or disclosure of PHI.
    b. Hawai'i HIE shall notify Subcontractor of any restriction on the use or disclosure of PHI that Hawai'i HIE has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Subcontractor's use or disclosure of PHI.

19. Subcontractor Obligations. Subcontractor may receive from Hawai'i HIE, or create or receive on behalf of Hawai'i HIE, health information that is protected under applicable state and/or federal law, including without limitation, PHI. Subcontractor agrees not to use or disclose (or permit the use or disclosure of) PHI in a manner that would violate the Confidentiality Requirements if the PHI were used or disclosed by Hawai'i HIE in the same manner. Subcontractor may use PHI for the proper management and administration of the Subcontractor or to carry out the legal responsibilities of Subcontractor. Subcontractor shall:
    a. comply with HIPAA Rules, and all applicable Regulations;
    b. use PHI in compliance with 45 CFR 164.504(e), except as otherwise required by law;
    c. not use or further disclose the information it obtains under this BAA other than as permitted or required by the BAA or as required by law;
    d. use appropriate safeguards and comply, where applicable, with 45 CFR Subpart C to prevent use or disclosure of the information other than as provided by the BAA; and
    e. report to Hawai'i HIE within five (5) days of Subcontractor becoming aware of any use or disclosure of the information not permitted in this BAA, including breaches of unsecured PHI as required by 45 CFR 164.410.

20. Disclosure of PHI. Subject to any limitations in this BAA, Subcontractor may disclose PHI to any third

party persons or entities as necessary to perform its obligations under this BAA, and as permitted or required by applicable federal or state law. Subcontractor may disclose PHI for the proper management and administration of Subcontractor or to carry out the legal responsibilities of the Subcontractor, provided the disclosures are required by law, or Subcontractor obtains reasonable assurances from the person or entity 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 or entity, and the person or entity notifies Subcontractor of any instances of which it is aware in which the confidentiality of the information has been breached. Subcontractor shall ensure that any person or entity that creates, receives, maintains, or transmits PHI on behalf of Subcontractor agrees to:

a. the same restrictions and conditions that apply to Subcontractor with respect to such information; and
b. comply with applicable requirements of 45 CFR Subpart C, including implementation of reasonable and appropriate safeguards to protect electronic PHI, by entering into a contract or other arrangement that complies with 45 CFR 164.314.
c. Subcontractor shall not use or further disclose PHI other than as permitted or required by this BAA or as required by law.

21. Duty to Mitigate. Subcontractor agrees to mitigate, to the extent practical and unless otherwise requested by Hawai'i HIE in writing, any harmful effect that is known to Subcontractor and is the result of a use or disclosure of PHI by Subcontractor (or any of Subcontractor's Authorized Users, agents or contractors) in violation of the Substantive Agreements including this BAA.

22. Individual Rights Regarding Designated Record Sets. Subcontractor shall:
    a. provide access to, and permit inspection and copying of, PHI by Hawai'i HIE on behalf of a covered entity or, as directed by a covered entity for which Subcontractor is obligated to comply as a business associate of Hawai'i HIE, an individual who is the subject of the PHI under conditions and limitations required under 45 CFR 164.524, as it may be amended from time to time;
    b. notify Hawai'i HIE within five (5) business days of receipt of any request for access or amendment by an individual; and
    c. make PHI that is part of an individual's designated record available for amendment by Hawai'i HIE on behalf of a covered entity or as directed by a covered entity for which Subcontractor is obligated to comply as a business associate of Hawai'i HIE under conditions and limitations required under 45 CFR 164.526, as it may be amended from time to time.

23. Accounting of Disclosures. Subcontractor shall make available in response to a request from an individual, information required for an accounting of disclosures of PHI for a period of up to six (6) years with respect to the individual in accordance with 45 CFR 164.528 and any related regulations or guidance issued by HHS in accordance with such provision.

24. Withdrawal of Authorization. Subcontractor agrees to cease the use and disclosure of an individual's PHI provided that:
    a. The Subcontractor's use or disclosure is based upon the patient's authorization for the use of the patient's PHI; and
    b. Subcontractor has notice from the Hawai'i HIE or patient that:
        i. the individual patient revokes such authorization in writing,
        ii. the effective date of such authorization has expired,

iii. the condition set forth in the authorization is no longer in effect or has expired, or
iv. the consent or authorization is found to be enforced in any manner that renders it invalid.

Nothing in this section is intended to require Subcontractor to cease the use or disclosure of PHI if Subcontractor has relied on such use or disclosure, where an exception under the Confidentiality Requirements expressly applies, or until clarification from the individual is received by Subcontractor if reasonably requested.

25. Records and Audit. Subcontractor shall make available to the HHS Secretary or its agents, for purposes of determining compliance with the HIPAA Rules, in a time and manner designated by the Secretary. Except to the extent prohibited by law, Subcontractor agrees to notify Hawai'i HIE within five (5) business days of its receipt of any and all requests by or on behalf of any and all federal, state and local government authorities served upon Subcontractor for PHI.

26. Indemnification. Indemnification shall be as set forth in the Substantive Agreements between Hawai'i HIE and Subcontractor. In the event the Substantive Agreements are silent regarding indemnification, the obligation to indemnify set forth in this section shall apply after any insurance, e.g. general liability or cybersecurity insurance, has been exhausted, or is determined by a court of competent jurisdiction not to afford coverage for a matter sought to be indemnified. The intent of this section is to allow insurance to respond to any claims before the obligation to indemnify activates for either Party to this Agreement.
    a. Subcontractor shall indemnify, defend and hold harmless Hawai'i HIE from and against any action brought by any third party against Hawai'i HIE with respect to any claim, action or demand, debt or liability, including reasonable attorney's fees, to the extent based on a breach or alleged breach of this Agreement, a violation or alleged violation of HIPAA (or other applicable healthcare confidentiality law) or any other law, alleged negligence or willful misconduct, or other alleged wrongdoing of Subcontractor or its own employees, agents or contractors. If Subcontractor assumes the defense of such a claim, Hawai'i HIE shall have the right, at its expense, to participate in the defense of such claim. Subcontractor shall not take any final action with respect to any such claim without the prior written consent of Hawai'i HIE, which consent shall not be unreasonably withheld. In the event of a breach of Unsecured Protected Health Information caused by Subcontractor, or its contractors and agents, Subcontractor shall indemnify Hawai'i HIE for the costs incurred by Hawai'i HIE to provide the notifications required by law.
    b. Hawai'i HIE shall indemnify, defend and hold harmless Subcontractor, its officers, employees and agents, from and against any action brought against the same by any third party or by any of Hawai'i HIE's Authorized Users, with respect to any claim, action or demand, debt or liability, including reasonable attorneys' fees, arising from or related to actions by Hawai'i HIE (or its own Authorized Users, employees, agents, or business associates, or contractors), to the extent that such action is based upon any claim of alleged breach of this Agreement, alleged violation of HIPAA or any other law, alleged negligence or willful misconduct, or other alleged wrongdoing of Hawai'i HIE (or its own Authorized Users, employees, agents, or business associates or contractors). If Hawai'i HIE assumes the defense of such a claim, Subcontractor shall have the right, at its expense, to participate in the defense of such claim. Hawai'i HIE shall not take any final action with respect to any such claim without the prior written consent of Subcontractor, which consent shall not be unreasonably withheld.

27. Compliance with the Security Rule. To the extent that Subcontractor creates, receives, maintains, or

transmits ePHI, Subcontractor shall also implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any ePHI that Subcontractor may create, receive, maintain or transmit on behalf of Hawai'i HIE in conformity with the requirements of the Security Rule. Subcontractor shall also implement policies and procedures and comply with documentation requirements in compliance with the Security Rule.

28. Implementation of Security Standards Notice of Security Incidents. Subcontractor acknowledges that it is required to comply with 45 CFR 164.308, 164.310, 164.312 and 164.316 as if Subcontractor were a covered entity, and Subcontractor agrees to comply with these provisions of the Security Standards. Furthermore, to the extent feasible, Subcontractor will use commercially reasonable efforts to ensure that the technology safeguards used by Subcontractor to secure PHI will render such PHI unusable, unreadable and indecipherable to individuals unauthorized to acquire or otherwise have access to such PHI in accordance with HHS Guidance published at 74 Federal Register 19006 (April 17, 2009), or such later regulations or guidance promulgated by HHS or issued by the National Institute for Standards and Technology ("NIST") concerning the protection of identifiable data such as PHI. Subcontractor shall report to Hawai'i HIE any Security Incident impacting Hawai'i HIE of which it becomes aware within five (5) business days. At a minimum, such report shall contain the following information to the degree that the information is known at the time of reporting:
    (i) date and time when the Security Incident occurred and/or was discovered;
    (ii) names of systems, programs, or networks affected by the Security Incident;
    (iii) preliminary impact analysis;
    (iv) description of and scope of ePHI used, disclosed, modified, or destroyed by the Security Incident; and
    (v) provide a report of any mitigation steps taken.

    Any Security Incident that is a Breach of Unsecured PHI shall be reported pursuant to Section 13.

29. Reporting of Privacy Incidents.

    13.1 Breach Notification to Hawai'i HIE and Mitigation. Subcontractor agrees to implement reasonable systems for the discovery and prompt reporting to Hawai'i HIE of any "breach" of "unsecured PHI" as those terms are defined by 45 CFR 164.402 or upon notice or any reasonable belief that a "breach" has occurred (hereinafter a "HIPAA Breach"). The Parties acknowledge and agree that 45 CFR 164.404, as described below in this section, governs the determination of the date of a Breach. In the event of any conflict between this Section and the Confidentiality Requirements, the more stringent requirements shall govern. Subcontractor will, following the discovery of a Breach, notify Hawai'i HIE immediately and in no event later than the first day (24 hours) after Subcontractor discovers such Breach, unless Subcontractor is prevented from doing so by 45 CFR 164.412 concerning law enforcement investigations. For purposes of reporting a Breach to Hawai'i HIE, the discovery of a Breach shall occur as of the first day on which such Breach is known to the Subcontractor or, by exercising reasonable diligence, would have been known to the Subcontractor. Subcontractor will be considered to have had knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the Breach) who is an employee, officer or other agent of the Subcontractor. No later than seven (7) business days following a Breach, Subcontractor shall provide Hawai'i HIE with sufficient information to permit Hawai'i HIE to comply with the Breach notification requirements set forth at 45 CFR 164.400 et seq. Specifically, if the following information is known to (or can be

reasonably obtained by) the Subcontractor, Subcontractor will provide Hawai'i HIE with:

(i) contact information for individuals who were or who may have been impacted by the Breach (e.g., first and last name, mailing address, street address, phone number, email address);

(ii) a brief description of the circumstances of the Breach, including the date of the Breach and date of discovery;

(iii) a description of the types of unsecured PHI involved in the Breach (e.g., names, social security number, date of birth, address(es), account numbers of any type, diagnostic and/or billing codes and similar information);

(iv) a brief description of what the Subcontractor has done or is doing to investigate the Breach, mitigate harm to the individual impacted by the Breach, and protect against future Breaches; and

(v) appoint a liaison and provide contact information for same so that the Hawai'i HIE may ask questions or learn additional information concerning the Breach.

Following a Breach, Subcontractor will have a continuing duty to cooperate with Hawai'i HIE regarding breach notification and inform Hawai'i HIE of new information learned by Subcontractor regarding the Breach, including but not limited to the information described in items (i) through (v), above.

13.2 Data Breach Notification and Mitigation under Other Laws. Subcontractor agrees that in the event any Individually Identifiable Information is lost, stolen, used or disclosed by Subcontractor (or its Recipients), and it is determined that such incident is in violation of one or more State data breach notification laws, Subcontractor shall promptly:

(i) cooperate and assist Hawai'i HIE with any investigation into any State Breach or alleged State Breach;

(ii) cooperate and assist Hawai'i HIE with any investigation into any State Breach or alleged State Breach conducted by HHS or any State Attorney General or State Consumer Affairs Department (or their respective agents) ;

(iii) comply with Hawai'i HIE's reasonable determinations regarding Hawai'i HIE's and Subcontractor's obligations to mitigate to the extent practicable any potential harm to the individuals impacted by the State Breach; and

(iv) assist with the implementation of any decision by Hawai'i HIE or any State or Federal agency, including, if necessary, HHS or any State Attorney General or State Consumer Affairs Department (or their respective agents), to notify individuals impacted or potentially impacted by a State Breach.

13.3 Cooperation of Subcontractor and Authority of Hawai'i HIE. Subcontractor will fully cooperate with Hawai'i HIE in any risk assessment conducted by Hawai'i HIE in order to determine whether any Breach compromises the security or privacy of the PHI. Subcontractor will accept Hawai'i HIE's final determination as to whether the PHI was compromised in any situation reported by Subcontractor to Hawai'i HIE.

30. Term and Termination.

14.1 Term. The Term of this BAA shall be effective as of the execution by signature of this BAA, and shall terminate in accordance with terms of this section or on the date Hawai'i HIE terminates for cause as authorized in section 14.2, whichever is sooner, provided, however, that termination shall not affect the respective obligations or rights of the parties arising under the

Substantive Agreements or this BAA prior to the effective date of termination, all of which shall continue in accordance with their terms.

14.2 Reasonable Steps to Cure Breach. If Hawai'i HIE learns of a pattern of activity or practice of Subcontractor that constitutes a material breach or violation of the Subcontractor's obligations under the provisions of this BAA, then Hawai'i HIE shall notify Subcontractor of the breach and Subcontractor shall take reasonable steps to cure such breach or end such violation, as applicable, within a period of time which shall in no event exceed thirty (30) days. If Subcontractor's efforts to cure such breach or end such violation are unsuccessful, Hawai'i HIE may terminate this BAA and applicable Substantive Agreements immediately upon written notice.

14.3 Hawai'i HIE shall have the right to terminate this BAA without cause upon ninety (90) days written notice to Subcontractor. Such termination of the BAA shall simultaneously terminate the Substantive Agreements on the same effective date, unless otherwise agreed to in writing by both parties.

14.4 Upon the termination of the Customer Agreement as part of the Substantive Agreements, this BAA will automatically terminate.

14.5 Upon termination of this BAA for any reason, Subcontractor agrees either to return to Hawai'i HIE or to destroy all PHI received from Hawai'i HIE or otherwise through the performance of services for Hawai'i HIE, that is in the possession or control of Subcontractor or its agents, unless return or destruction is not feasible or lawful, or unless other legal grounds exist for retaining the PHI. In the case of PHI which is not returned or destroyed, Subcontractor shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, or as otherwise permitted by law, for so long as Subcontractor maintains such PHI. Subcontractor further agrees to comply with other applicable state or federal law, which may require a specific period of retention, redaction, or other treatment of such PHI.

31. Ineligible Persons. Subcontractor represents and warrants to Hawai'i HIE that Subcontractor (i) is not currently excluded, debarred, or otherwise ineligible to participate in any federal health care program as defined in 42 USC § 1320a-7b(f) ("the Federal Healthcare Programs"); (ii) has not been convicted of a criminal offense related to the provision of health care items or services and not yet been excluded, debarred, or otherwise declared ineligible to participate in the Federal Healthcare Programs, and (iii) is not under investigation or otherwise aware of any circumstances which may result in Subcontractor being excluded from participation in the Federal Healthcare Programs. This shall be an ongoing representation and warranty during the term of this BAA, and Subcontractor shall immediately notify Hawai'i HIE of any change in the status of the representations and warranty set forth in this section. Any breach of this section shall give Hawai'i HIE the right to terminate this BAA immediately for cause.

32. Miscellaneous.

16.1 Notices. All notices, requests, demands and other communications required or permitted to be given or made under this BAA shall be in writing, shall be deemed to have been duly given if transmitted by email or delivered by facsimile, courier service, or personal delivery to the addresses or email addresses listed below, in each case with verification or

acknowledgement of delivery, or three (3) days after mailing first class, postage prepaid, return receipt requested, to such address. Hawai'i HIE and Subcontractor may change their own address or email address for purposes of this section by giving the other written notice of the new address or email address.

| If to Hawai'i HIE, to: | If to Subcontractor, to: |
|---|---|
| 900 Fort Street Mall, Suite 1305<br>Honolulu, Hawai'i 96813 | _____<br>_____ |
| Attention: Christine Sakuda | Attention: _____ |
| E-mail: csakuda@hawaiihie.org | Email: _____ |

16.2 Waiver. No provision of this BAA or any breach thereof shall be deemed waived unless such waiver is in writing and signed by the Party claimed to have waived such provision or breach. No waiver of a breach shall constitute a waiver of or excuse any different or subsequent breach.

16.3 Assignment. Neither Party may assign (whether by operation or law or otherwise) any of its rights or delegate or subcontract any of its obligations under this BAA without the prior written consent of the other Party. Notwithstanding the foregoing, Hawai'i HIE shall have the right to assign its rights and obligations hereunder to any entity that is an affiliate or successor of Hawai'i HIE, without the prior approval of Subcontractor.

16.4 Severability. Any provision of this BAA that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this BAA or affecting the validity or enforceability of such remaining provisions unless such severance makes the remaining provisions of this BAA impractical to perform, in which case the BAA is terminated.

16.5 Governing Law. This BAA shall be governed by and interpreted in accordance with the laws of the State of Hawai'i, excluding its conflicts of law's provisions, except insofar as governed by federal law (such as HIPAA).

16.6 Equitable Relief. Notwithstanding the Parties' duty to arbitrate all other claims, the Parties understand and acknowledge that any disclosure or misappropriation of any PHI in violation of HIPAA or in violation of this BAA may cause the other Party irreparable harm, the amount of which may be difficult to ascertain, and therefore agrees that any Party shall have the right to apply to a court of competent jurisdiction in Hawai'i for specific performance and/or an order restraining and enjoining any such further disclosure or breach and for such other emergency relief as the Party may deem appropriate, reserving all other claims for binding arbitration, in accordance with the provisions of the Substantive Agreements. Such rights are to be in addition to the remedies otherwise available at law or in equity. The Parties expressly waive the defense that a remedy in damages will be adequate and further waive any requirement in an action for specific performance or injunction for the posting of a bond.

16.7 Nature of Agreement; Independent Contractor. Nothing in this BAA shall be construed to create (i) a partnership, joint venture or other joint business relationship between the parties

or any of their affiliates, or (ii) a relationship of employer and employee between the parties. Subcontractor is an independent contractor, and not an agent of Hawai'i HIE. This BAA does not express or imply any commitment to purchase or sell goods or services.

16.8 Interpretation, Changes in Law. Any ambiguity in this BAA shall be resolved to permit the Parties to comply with the HIPAA Rules.

| **Hawai'i HIE** | **Subcontractor** |
|---|---|
| By: Christine Sakuda | By: _____ |
| Title: Executive Director | Title: _____ |
| _____ | _____ |
| Signature | Signature |
| Date: _____ | Date: _____ |
| Phone: 808-441-1313 | Phone: _____ |
| Email: csakuda@hawaiihie.org | Email: _____ |