TITLE: Incident Response and Mitigation	
Policy #: HEN-012	Effective Date: July 17, 2013
Program: Hawai'i HIE	Revision Date: November 15 , 2016
Approved By: Hawai'i HIE Board of Directors	

Table of Contents

1. Purpose

This policy provides requirements for identifying and mitigating events that potentially compromise: 1) the privacy and/or security of Confidential Information entrusted to the Hawai'i HIE and Health eNet Participants, and/or 2) the proper functionality of the Hawai'i HIE's Health eNet system ("Health eNet", the "System").

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

Confidential Information. Personally Identifiable Information, Protected Health Information and Proprietary Information, as defined below:

- Personally Identifiable Information (PII) – Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual.
- Protected Health Information (PHI) – Healthcare-related information about an individual within the scope of HIPAA. PHI is a subset of PII.
- Proprietary Information – Non-public Information, other than PII, that is the property of the Hawai'i HIE or Health eNet Participants, including but not limited to: trade secrets, plans, designs, research and development, pricing, new product and marketing plans, programming codes, and financial information.

Incident. An event involving an unauthorized activity related to Confidential Information or the Health eNet's functionality such as, but not limited to, the following:

- Privacy Incident – An event involving unauthorized access, use, or disclosure of PII, whether in oral, hardcopy or electronic form.
- Security Incident – An event involving an unauthorized attempt to access, use, obtain, disclose, modify, or destroy electronic information within or via the Health eNet; and/or to tamper with the functionality of the System. An event can represent a Security Incident concurrent with a Privacy Incident. Unauthorized unsuccessful attempts to compromise the System's security, e.g. firewall pings, may not be construed as Security Incidents.

4. Policy

The Hawai'i HIE and Health eNet Participants will implement policies and procedures for establishing communications in response to events that are potential Incidents; mitigating the adverse effects of Incidents; and providing notifications regarding Incidents as required by federal and state laws.

4.1. Incident Response Team. The Hawai'i HIE will maintain an Incident Response Team (IRT) consisting of, at a minimum, the Hawai'i HIE's Compliance and Privacy Officer, Security Officer and Director of IT Operations.

Procedures
1. The Hawai‘i HIE shall appoint its Compliance and Privacy Officer, Security Officer and Director of IT Operations as standing members of the IRT.
2. The IRT may evaluate the need for, and appoint additional standing team members from the Hawai‘i HIE’s workforce, based on trend analysis of historical Incidents.
3. To investigate and mitigate a given Incident, the IRT and involved Participants may appoint or request the assistance of persons who are not HHIE workforce members, e.g. Participants’ and subcontractors’ designated Privacy Officers, Security Officers and / or other Incident Response Points of Contact.

4.2. Discovering and Reporting of Potential Incidents.

4.2.1. Discovery by Hawai‘i HIE’s Workforce Members, or Hawai‘i HIE’s Business Associates or Subcontractors. A Hawai‘i HIE workforce member, BA or subcontractor that discovers or receives a complaint or other notification about, or is responsible for a potential Incident must immediately report the event to the Hawai‘i HIE’s Compliance and Privacy Officer or other member of the IRT.

Procedures
1. A Hawai‘i HIE workforce member, BA or subcontractor (Discovering Party) discovers an Incident, or receives a complaint and/or notification that may be related to an Incident.
2. Discovering Party shall immediately report the incident to the Hawai‘i HIE Compliance and Privacy Officer or other member of the IRT.
3. The IRT member initially made aware of the Incident or complaint / notification will create an initial Incident report as soon as possible after becoming aware of the Incident or complaint / notification. The Incident report will be entered in the Hawai‘i HIE’s Incident management and tracking system, and updated as necessary by the IRT, in accordance with HIPAA and other applicable laws’ documentation requirements.

4.2.2. Discovery by Participant’s Workforce Members, or Participant’s Business Associates or Subcontractors. Each Participant shall establish procedures for reporting potential Incidents to a Privacy Officer, Security Officer or other Incident Response Point of Contact designated by the Participant. A Participant that becomes aware of a potential incident involving the Health eNet, or Confidential Information belonging to or entrusted to the Hawai‘i HIE, must immediately report the event to the Hawai‘i HIE.

4.2.2.1. Potential Incident for Which Participant’s Workforce Member, or Participant’s Business Associate or Subcontractor May Be Responsible.

Procedures
1. A Participant discovers an Incident involving the Health eNet or Confidential Information belonging to or entrusted to the Hawai‘i HIE.

2. The Participant's Privacy Officer, Security Officer, or other Incident Response Point of Contact designated by the Participant shall conduct an investigation, an Incident risk assessment and mitigations regarding the Incident, according to the Participant's policies and procedures.
3. The Participant notifies the Hawai'i HIE of substantiated Incident within thirty (30) days of discovery by the Participant, and includes the following information in the notification: 1) Date and time of Incident (e.g. unauthorized access, based on audit data); 2) Identity of the individual whose information was accessed, used or disclosed in an unauthorized manner; 3) Description of information accessed, used or disclosed in an unauthorized manner; 4) Name of Participating Organization responsible for Incident; 5) Address of Participating Organization responsible for incident; 6) Name of Primary Point of Contact for Participating Organization responsible for incident; 7) Whether or not the Participating Organization responsible for the incident did, or intends to do a breach notification to the individual, if known at the time the Participant notifies the Hawai'i HIE. Refer to and follow steps listed below in subsection 4.2.4, "Options for Reporting to the Hawai'i HIE", regarding acceptable methods of submission of information to Hawai'i HIE Community Relations.

4.2.2.2. Potential Incident for Which the Participant Is Not Responsible.

Procedures
1. A Participant discovers an Incident involving the Health eNet or Confidential Information belonging to or entrusted to the Hawai'i HIE.
2. The Participant's Privacy Officer, Security Officer, or other Incident Response Point of Contact designated by the Participant shall immediately report discovery of the potential Incident to the Hawai'i HIE's Compliance and Privacy Officer or other member of the IRT. A. Participant shall notify Hawai'i HIE and provide the following information: 1) Date and time of incident (e.g. unauthorized access, based on audit data); 2) Identity of the individual whose information was accessed, used or disclosed in an unauthorized manner; 3) Identity(ies) of the person(s) who is/are allegedly responsible for the potential Incident;

4) If a person allegedly responsible for a potential Incident is a Health eNet Authorized User, identity of the User's Participating Organization, if known; 5) Description of unauthorized access, use or disclosure of Confidential Information. 6) Contact information, e.g. phone number and / or email address, of the Reporting Party. B. Refer to and follow steps listed below in subsection 4.2.4, "Options for Reporting to the Hawai'i HIE", regarding acceptable methods of submission of information to Hawai'i HIE Community Relations.
3. The IRT then undertakes an analysis of the incident, as described in section 4.3.1.
4. Refer to subsection 4.6 for documentation requirements by a Participant.

4.2.3. Discovery by Individuals and Other Reporting Parties. In the event an individual or other Reporting Party (e.g. an individual's personal representative, a person or organization that is not the Hawai'i HIE, a Participant, or a workforce member of the Hawai'i HIE, a Participant, or any of their subcontractors) reports a potential incident to the Hawai'i HIE, the Hawai'i HIE will undertake the following procedure steps.

Procedures
1. Reporting Party discovers a potential Incident involving the Health eNet or Confidential Information belonging to or entrusted to the Hawai'i HIE.
A. When a Reporting Party notifies the Hawai'i HIE, the Hawai'i HIE will attempt to obtain the following information from the Reporting Party: 1) Date and time of incident (e.g. unauthorized access, based on audit data); 2) Identity of the individual whose information was accessed, used or disclosed in an unauthorized manner; 3) Identity(ies) of the person(s) who is/are allegedly responsible for the incident; 4) If a person allegedly responsible for an incident is a Health eNet Authorized User, identity of the User's Participating Organization, if known; 5) Description of unauthorized access, use or disclosure of Confidential Information. 6) Contact information, e.g. phone number and / or email address, of the Reporting Party. B. Refer to and follow steps listed below in section 4.2.4, "Options for Reporting to the Hawai'i HIE", regarding acceptable methods of submission of information to Hawai'i HIE Community Relations.

2. The IRT will then undertake an analysis of the incident, as described in section 4.3.1.

4.2.4. Options for Reporting Incidents to the Hawai‘i HIE. The Hawai‘i HIE will provide methods by which a Participant, individual or other Reporting Party may report a potential Incident to the Hawai‘i HIE.

Procedures
1. The Hawai‘i HIE provides the following methods for reporting a potential incident, to the attention of Hawai‘i HIE “Community Relations”: 1) Phone (the Community Relations team will attempt to obtain the information required in steps 4.3.2.A, steps 1-6 above). If the Reporting Party is a Participant, a written report should be provided to the Hawai‘i HIE following the phone call that includes a transcription of the phone call details 2) Secure online form* on the Hawai‘i HIE's website 3) Secure e-mail* 4) Notifications sent to the Hawai‘i HIE via other means, e.g. fax, e-mail, U.S. Postal Service, or other delivery service, should be addressed to the Hawai‘i HIE "Community Relations" team, which will then forward the notification to a member of the Hawai‘i HIE Incident Response Team 5) Written notifications should be mailed/delivered by first-class U.S. mail, with a form of delivery confirmation, to: Community Relations Hawai'i Health Information Exchange 900 Fort Street Mall, Suite 1305 Honolulu, HI 96813 * Messages from HIPAA covered entity Participants must be secured (e.g. via encryption) as required by federal specifications referenced in 45 CFR Subpart C if the message includes electronic PHI.

4.3. Incident Response and Mitigation. Upon receiving a report of a potential Incident, the Incident Response Team will analyze and investigate the event and begin taking actions to mitigate any adverse effects of the event.

If the event involves, or likely involves theft or other criminal activities, the Hawai‘i HIE will report the Incident to the appropriate law enforcement agency.

The Incident Response Team will determine whether or not the event potentially adversely affects or otherwise involves any Participants. If the event involves a Participant, the Hawai‘i HIE will promptly notify the Participant of the event, unless a law enforcement agency imposes a restriction on doing so according to applicable laws. An involved Participant will designate its Incident Response Point of Contact, or one or more other member of its workforce, to participate in the investigation as part of the Incident Response Team.

4.3.1. Hawai‘i HIE Incident Analyses.

Procedures
1. In the event the Hawai‘i HIE receives a report about an Incident or potential Incident from a Participant, individual or reporting party that has not already been substantiated by a Participant*, the Hawai‘i HIE IRT conducts a preliminary analysis of the information provided by the Reporting Party to help determine if the event poses a risk to Confidential Information, and which Participant(s) may be impacted (e.g. as a party responsible for, or potentially harmed by, the event). In the event the preliminary analysis determines that one or more Participants may be impacted by the Incident, the Hawai‘i HIE will provide its preliminary analysis to the Participant(s), in accordance of the terms of the BA agreement(s) between the Participant(s) and Hawai‘i HIE. Participant(s) may use the preliminary analysis to help conduct Incident investigations (subsection 4.3.3) and Incident risk assessments (subsection 4.3.4), as required by HIPAA and / or state law. * In the event of an Incident for which a Participant’s workforce member, BA or subcontractor may be responsible (subsection 4.2.2.1 above), if the incident is substantiated, then the Participant completes the Incident risk assessment and does not rely on analysis by the IRT.
2. If during the analysis the Incident is determined to be substantiated, the Hawai‘i HIE IRT will commence mitigation of adverse effects of the Incident based on the analysis.
3. If the Hawai‘i HIE Compliance and Privacy Officer or IRT is directed by law enforcement not to notify Participant(s) of a reported incident and/or its adverse effects, then the Hawai‘i HIE Compliance and Privacy Officer or IRT shall comply with law enforcement directives, to the degree they adhere to HIPAA and other applicable laws’ standards regarding suppression of notifications to the Participant(s).

4.3.2. Incident Notifications to the President of the Hawai‘i HIE’s Board of Directors.

Procedure
1. The IRT will notify the President of the Hawai‘i HIE Board of Directors of any potential Incidents impacting a significant number of participants and / or individuals, or security compromise of the Health eNet.

4.3.3. Incident Investigations.

Procedures
1. Upon receipt of notification from the IRT of reported Incident and/or adverse effects, potentially impacted Participant(s) will designate an Incident Response Point of Contact, or one or more other members of its workforce,

to participate in the investigation as part of the IRT.
2. The IRT will determine, based on the investigation, if an Incident is substantiated, unsubstantiated, or cannot be definitively substantiated or unsubstantiated (i.e. the results of the investigation are inconclusive).
3. The Participant will also follow its established internal procedures for participation in Incident investigation.
4. Hawai‘i HIE IRT will devise a mitigation plan to address Incident, and risks and adverse effects associated with the Incident.

4.3.4. Incident Risk Assessments. If the Incident is substantiated, or the investigation otherwise indicates potential privacy or security risks, the Incident Response Team will conduct an Incident risk assessment to identify any such risks and implement additional reasonable mitigations to address the risks.

Procedures
1. Participants impacted by the Incident will also follow their respective established internal procedures to determine if a risk assessment is necessary, and if so conduct the risk assessment, e.g. to determine if HIPAA Breach notifications (see subsection 4.4.3.2) and other mitigations are required.
2. In the event the Hawai‘i HIE is responsible for a substantiated Incident that involves “personal information” as defined at Hawaii Revised Statutes 487N, e.g. a State Breach (see subsection 4.4.3.3), the Hawai‘i HIE IRT shall conduct a risk assessment to determine if Breach notifications and other mitigations are required.

4.4. Notifications Regarding Substantiated Incidents. In the event an Incident, whether it qualifies as a “Breach” as described in this section, is substantiated, the Hawai‘i HIE and Participants shall provide notifications, as necessary under federal and state laws.

4.4.1. Incident Notifications to the Hawai‘i HIE’s Executive Director.

Procedure
1. The IRT will notify the Hawai‘i HIE Executive Director of any substantiated Incidents for which the Hawai‘i HIE is responsible, and any incidents that, in the Hawai‘i HIE IRT’s professional judgment, require the Executive Director’s attention, e.g. for the purposes of communications to involved participants, or media relations.

4.4.2. Incident Notifications to Law Enforcement Agencies.

Procedure
1. In the event the Incident involves, or likely involves, theft or other criminal activities, the Hawai‘i HIE will notify the appropriate law enforcement agency about the Incident.

4.4.3. Breach Notifications. The Incident Response Team, in collaboration with the involved Participant(s), will determine if a Privacy Incident or Security Incident qualifies as a breach of unsecured PHI, as defined in 45 CFR §164.402, and/or a breach of PII under one or more state laws ("State Breach").

4.4.3.1. Notifications to the Hawai'i HIE's Board of Directors.

Procedure
1. The IRT will notify the President of the Board of Directors of any substantiated Breaches for which the Hawai'i HIE is responsible, including a summary of the Incident and analysis, and the mitigation plan, within seventy-two (72) hours of Incident reporting.

4.4.3.2. HIPAA Breach Notifications.

If an Incident qualifies as a breach of unsecured PHI, the Hawai'i HIE shall provide information for the Participant to make required notifications regarding the breach to the impacted individual(s), the media, and/or the Secretary of the Department of Health and Human Services.

Procedures
1. A Participant that is a covered entity under HIPAA determines that an Incident qualifies as a HIPAA Breach, and that the Participant is responsible for providing notifications to the impacted individual(s), the media, and/or the Secretary of the Department of Health and Human Services (in accordance with 45 CFR §164.404, §164.406, §164.408 and §164.410).
2. The Hawai'i HIE will provide information for the Participant to make the required notifications regarding the Breach. The Hawai'i HIE may provide additional support for the Participant to make the required notifications regarding the Breach.
3. The Participant shall follow its internal policies and procedures for providing HIPAA Breach notifications.

4.4.3.3. State Breach Notifications.

Procedure
1. The Hawai'i HIE shall provide notifications as required under applicable state laws for Incidents, e.g. "Security Breaches", as defined in Hawaii Revised Statutes §487N.

4.5. Other Incident and Breach Mitigations.

Procedures
1. The IRT will determine what additional mitigations, if any, are required or necessary to address a given Incident.

The Hawai‘i HIE will implement any such mitigations for which it is determined to be accountable by the IRT.
2. Participants will follow their established internal procedures for determining and implementing any additional mitigations beyond the scope of mitigations determined by the Hawai‘i HIE IRT, if necessary.

4.6. Incident Documentation. The Hawai‘i HIE will maintain documentation related to potential and substantiated Incidents, including risk assessments and mitigation activities. The documentation for a given event will be retained for a minimum of six (6) years, and may include dates, names of involved parties and other pertinent information.

Participants that are covered entities may request information within such documentation as necessary to fulfill a request by an individual for an accounting of disclosures of that individual's PHI, as required by HIPAA. Please see the Hawai‘i HIE's *Individual Rights* policy for additional information about accountings of disclosures.

Procedures
1. Hawai‘i HIE Incident Response Team (IRT) will document all potential and substantiated Incidents in the Hawai‘i HIE's incident tracking system.
2. The documentation for a given event will be retained for a minimum of six (6) years, subject to requirements in federal and state law, and the BA agreements between the Hawai‘i HIE and Participants. The documentation may include but is not limited to: dates, names of involved parties and other pertinent information.
3. Records will be stored in a secure manner, in compliance with 45 CFR Subpart C.
4. Participants shall follow their respective internal procedures for documentation of Incident and Breach response, mitigation and notification.

4.6.1. Periodic Reporting to the Hawai‘i HIE Board of Directors. The Hawai‘i HIE Compliance and Privacy Officer will periodically report information summarizing incident and breach metrics to the board of directors.

Procedure
1. The Compliance and Privacy Officer will provide an incident report to the board of directors at a minimum on a quarterly basis. Such incident reports may include, among other information deemed relevant by the board of directors: the number of participants impacted, by a given incident or in aggregate; the number of individuals impacted, by a given incident, in aggregate, and / or by category of incident / violation.

4.7. Non-Retaliation. The Hawai‘i HIE will not take any retaliatory actions against any individual or entity that reports an Incident or suspected Incident.

4.8. Hawai‘i HIE Workforce Sanctions. The Hawai‘i HIE shall sanction a member of its workforce responsible for an Incident, as required by HIPAA.

4.9. Consequences for Hawai‘i HIE Subcontractors and Participants Related to Incident and Breach Mitigation.

- The Hawai‘i HIE shall take appropriate mitigating measures against a Health eNet User or Hawai‘i HIE subcontractor responsible for an Incident, as provided for by the Hawai‘i HIE’s policies and procedures and applicable contracts.
- The BA agreement between the Hawai‘i HIE and a Health eNet Participant will determine recourse in the event the Participant is responsible for an Incident.
- Participants shall adhere to their respective policies and procedures regarding sanctions of their workforce members.

5. Revision History

Revision Date	Revision Type*	Author(s)	Revision Rationale, Description	Approved by
July 19, 2013	New	Legal/Policy Committee (policy sub-committee)	Initial version of policy	Hawai‘i HIE Board of Directors
Nov 15, 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)