TITLE: HIE System Audit	
Policy #: HEN-010	Effective Date: April 4, 2012
Program: Hawai'i HIE	Revision Date: May 18, 2016
Approved By: Hawai'i HIE Board of Directors	

Table of Contents

1. Purpose

The purpose of this policy is to prevent/limit unauthorized access, use and disclosure of protected health information (PHI) via the Hawai'i HIE Health eNet system ("Health eNet", the "System"), and to ensure that Authorized Users are adhering to Hawai'i HIE operational policies and procedures, and applicable state and federal laws.

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

Audit. For the purposes of this policy, an audit is an evaluation of data or other information pertaining to Health eNet User activity, the User population itself, or operational processes associated with the System, to identify potential security risks, and to ensure that only individuals with a current need to use the System have access to the System.

Audit Log. A record of computing application or system activity (e.g. within the Health eNet) and/or of user activity of an application or system.

Audit Report. A report based on data stored within audit logs utilized in the course of implementing security safeguards, e.g. system activity review and audit, incident response and mitigation. Audit reports are retained in accordance with HIPAA and other applicable laws.

4. Policy and Procedures

The Hawai'i HIE and Participants shall conduct audits to ensure Authorized Users of the System are adhering to Hawai'i HIE operational policies and procedures, and applicable state and federal laws; e.g. helping prevent/limit unauthorized access, use and disclosure of protected health information (PHI) via the Hawai'i HIE Health eNet System.

The Hawai'i HIE will maintain audit logs of Participants contributing information to the Health eNet and Authorized Users accessing information via the System. Audit logs will be available upon request, or directly through the System, to Hawai'i HIE staff, Participants and individuals, for purposes provided for in this and other Hawai'i HIE Operational Policies.

Per 45 CFR § 164.316(b)(2)(ii), Hawai'i HIE shall make its audit reports available to those Hawai'i HIE and Participants' personnel responsible for audit implementation and management, and shall maintain audit report documentation in such a manner that it reflects the current status of security plans and procedures implemented to comply with the HIPAA Security Rule.

4.1. Audits of System Access by Users

Access Audits by Participants. Upon request by a Participant (e.g. the organization's management, Privacy Officer or Security Officer) to fulfill its auditing and monitoring obligations under HIPAA, the Hawai'i HIE shall run access audit reports as frequently as required by the Participant's policies and procedures, or for the prior month at a minimum. The Participant will be responsible for reviewing the reports to determine if any unauthorized access, use or disclosure of information by that Participant's Users has occurred.

Procedures
1. Participant Auditor requests Health eNet system access reports from the Hawaii HIE (which currently serves as the Site Administrator for all Health eNet participants).
2. The Hawai'i HIE runs system access reports, as requested in Step 1. The reports may include, but not be limited to the following information: • Date and time of access; • Identity of the Authorized User accessing the information; • Identity of the Authorized User's Participating Organization; • Locations (i.e. IP addresses) that indicate via which network components an access event occurred, if available; • Identity of each patient whose information was accessed; • Type of information, record, or section of record accessed (e.g. pharmacy data, laboratory data, document type); • Event type (e.g. view, print); • Whether the access was routine or a Access Additional Records (formerly "Break Glass") event;

• Access Additional Records reason, if applicable; and • Source or location where the information is stored.
3. Participant Auditor reviews system access reports, identifying any potential unauthorized access, use or disclosure of information by Participant's Users.
4. Participant notifies the Hawai'i HIE, and conducts and documents incident response activities related to any identified unauthorized access, use or disclosure of information, per Participant's policies and procedures (please refer to Hawai'i HIE HEN-012, *Incident Response and Mitigation* Operational Policy and Procedures).

Access Audits by the Hawai'i HIE. The Hawai'i HIE will run ad hoc access audit reports for one or more Participants, and work with those Participants to determine if any unauthorized activity has occurred.

Procedures
1. Hawai'i HIE will choose five (5) percent or more of records accessed across Participant community at least once every ninety (90) days.
2. Hawai'i HIE will run system access reports, as requested in Step 1. The reports shall include, but not be limited to the information specified in Access Audits by Participants, Step 2, in the preceding section.
3. Participant reviews system access reports, identifying any potential unauthorized access, use or disclosure of information by Participants' Users (please refer to Audit Criteria of the Audits for Monitoring of Participant and User Activity section below).
4. The Hawai'i HIE creates report of potential security incidents and provide the report to the Participant for review and identification of any unauthorized access, use or disclosure of information.
5. Participant notifies the Hawai'i HIE, and conducts and documents incident response activities related to any identified unauthorized access, use or disclosure of information, per Participant's policies and procedures (please refer to Hawai'i HIE HEN-012 *Incident Response and Mitigation* Operational Policy and Procedures).

4.2. Audits of Active Authorized Users. On a periodic basis, the Hawai'i HIE will run reports listing all active Authorized Users for each Participant. Each report will contain User names, access roles and last access dates, and will be sent to the Participant.

Procedures
1. The Hawai'i HIE runs active report listing Authorized Users for a Participant, at a minimum of once every year,. Each report will contain User names, access roles and last access dates.
2. The Hawai'i HIE and Participant review report listing active Authorized Users to Participant's Primary Point of Contact.
3. Participant determines if any Users' access authorities need to be: • Modified, due to a change in job function or duties; • Suspended, e.g. due to a leave of absence or an investigation of alleged unauthorized access, use or disclosure of information via the Health eNet; or • Terminated, e.g. due to the User no longer being part of the Participant's workforce or disciplinary reasons.
4. The Hawai'i HIE modifies, suspend and/or terminate Users' access authorities as

directed by Participant's Primary Point of Contact, according to the Modification of User Access and Leaves of Absence provisions in the Hawai'i HIE HEN-005 *Access Management* Operational Policy and Procedures.
5. Participant Primary Point of Contact reports confirmation of completion of Authorized Users audit to the Hawai'i HIE, including the date of audit completion.

4.3. Audits of Site and System Administrators' Activity. The Hawai'i HIE shall maintain audit logs of Site and System Administrators' activity, including but not limited to creation, modification, suspension and termination of Authorized Users' accounts.

Procedures
1. The Hawai'i HIE will run audit report(s) of activity by not less than twenty-five (25) percent of Authorized Users with administrative Health eNet privileged access. Each report will contain, but not be limited to the following information: • Date and time of access; • Identity of the administrative User accessing the information; • Identity of the administrative User's Participating Organization (if applicable); • Identity of each Authorized User whose information was accessed by the administrative User; and • Actions/changes implemented by the administrative User.
2. Hawai'i HIE's management reviews audit report(s), identifying any potential errors (including failures to execute necessary actions/changes, creation of unauthorized accounts), or security incidents by administrative Users, at a minimum once every ninety (90) days.
3. Conduct and document correction of any errors, taking into consideration provisions of Hawai'i HIE HEN-005 *Access Management* Operational Policy and Procedures.
4. The Hawai'i HIE notifies any impacted Participant(s), and conduct and document incident response activities related to any identified security incidents, per Participant's policies and procedures (please refer to Hawai'i HIE's HEN-012 *Incident Response and Mitigation* Operational Policy and Procedures).

4.4. Reports of Ambiguous or Potentially Duplicate Records. The Hawai'i HIE may create, maintain, and share reports of ambiguous (e.g. lack of data required for reliable matching) or potentially duplicate records with Participants. Each report provided to a given Participant will identify the anomalies in the records contributed by that Participant.

Procedures
1. The Hawai'i HIE reviews audit reports that identify the source of data for duplicative or ambiguous data.
2. The Hawai'i HIE conducts and documents correction of any errors, in accordance with the Hawai'i HIE HEN-008 *Individual Rights* – Amendments Operational Policy and Procedure, and HEN-005 *Access Management* Operational Policy and Procedures.
3. The Hawai'i HIE will notify Participant of need for correction in accordance with Hawai'i HIE HEN-008 *Individual Rights* – Amendments Operational Policy and Procedures.
4. The Hawai'i HIE will document incident response activities related to any identified data integrity issues, in accordance with Hawai'i HIE HEN-012 *Incident Response and*

Mitigation Operational Policy and Procedures.

4.5. Audits for Monitoring of Participant and User Activity. The Hawai'i HIE may conduct periodic audits (at least annually) to determine if Participating Organizations' Users are compliant with Hawai'i HIE operational policies

Procedures

1. The Hawai'i HIE will conduct periodic audits (at least annually) to determine if Participating Organizations' Users are compliant with Hawai'i HIE operational policies.
2. Audit criteria will include but are not limited to:
   - Opt-Out and Opt-Back-In Documents – Determine whether or not the documents are on file for patients who have requested a change in their Health eNet Community Health Record participation statuses;
   - Access Additional Records – Determine whether or not Users that accessed information through the Access Additional Records function went on to establish a patient relationship;
   - Role-Based Authorizations – Determine which roles have designated for each Authorized User;
   - Anomalous Patterns of User Activity – Anomalies may include: excessive queries; excessive Access Additional Records attempts; and excessive log-in failures. As patterns are identified and anomalous behavior becomes more apparent in the monthly audit reports, Hawai'i HIE may establish thresholds for each type of activity captured in the audit report.

   In addition, reports for anomalous patterns of user activity may include, but are not limited to:
   - Access Additional Records Trending – Monitoring the number of times a User accessed records using Access Additional Records. The Hawai'i HIE may flag a User account if the Access Additional Records count exceeds established thresholds.
   - Pediatric Specialty Practices – If a practice is listed as a pediatric specialty, the Hawai'i HIE monitors for Access Additional Records access when the patient is over the age of eighteen (18) years old.
   - Adult Special Practices – If a practice is listed as an adult specialty, the Hawai'i HIE monitors for Access Additional Records access when the patient is under the age of eighteen (18) years old.
   - Gynecological and Obstetrics/Gynecological (OB/GYN) Specialty Practices – If a practice is listed as a GYN or OB/GYN specialty, the Hawai'i HIE monitors for Access Additional Records access when the patient is a male.
   - Geriatric Specialty Practices – If a practice is listed as a geriatric specialty, Hawai'i HIE monitors for Access Additional Records access when the patient is under the age of fifty (50) years old.
   - Same Last Name – Monitoring for Same Last Name access when Users and patients have the same last name.
   - After Hours Access – Monitoring for After Hours Access for accessing Health eNet after regular business hours.
   - Questionable Location of Access - Monitoring for any access to Health eNet at locations other than where user is authorized.

3. Reports will be reviewed by the Hawai'i HIE Compliance and Privacy Officer within thirty (30) days of generating audit reports.

4.6. Audit Findings Indicating Unauthorized Access, Use, or Disclosure. A Participant shall immediately notify the Hawai'i HIE whenever the Participant detects or suspects an unauthorized access, use or disclosure of information via the Health eNet.

In the event the Hawai'i HIE detects or suspects unauthorized access, use or disclosure of information via the Health eNet, the Hawai'i HIE shall immediately notify any Participant that is associated with a User that is or may be responsible for such unauthorized activity.

Procedures
1. Participant detects or suspects unauthorized access, use or disclosure of information via the Health eNet.
2. Participant and the Hawai'i HIE shall follow the provisions of the Hawai'i HIE HEN-012 *Incident Response and Mitigation* policy and procedure to investigate the alleged unauthorized activity and take additional corrective actions if needed.

4.7. Immutability of Audit Logs. Audit logs shall be immutable. An immutable audit log requires either that log information cannot be altered by anyone regardless of access privilege or that any alterations are tamper evident.

Procedures
1. The Hawai'i HIE shall ensure that their audit logs are immutable and therefore unalterable by anyone regardless of access privilege.
2. The Hawai'i HIE shall ensure that their audit logs are also tamper evident in the event that alterations have been made.
2. Selection of audit reporting software and subsequent upgrades or changes to existing software shall ensure continuation of immutability and tamper evidence of audit logs.

4.8. Retention.

4.8.1. Audit Reports. Audit reports shall be retained for a period of time equal to or greater than the minimum length of time specified by HIPAA[1] and other applicable laws, based on which length of time specified by law is greater.

Procedure
1. A. The Hawai'i HIE shall retain audit reports for a period of at least (6) years. B. Audit reports shall be retained in electronic and/or printed form and included in the Hawai'i HIE's data back-up plan.

[1] Documentation requirements guidance provided by the U.S. Office for Civil Rights: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf

4.8.2. Audit Logs. Audit logs shall be retained by the Hawai'i HIE.

Procedure
1. A. The Hawai'i HIE shall retain audit logs for a period of one (1) year to three (3) years. B. Audit logs shall be retained in electronic and/or printed form and included in the Hawai'i HIE's data back-up plan.

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
June 2, 2014	Amendment	Legal/Policy Committee	New definitions added, edits to language related to audit reports and audit report retention	Hawai'i HIE Board of Directors
May 18, 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)