

TITLE: Audit	
Policy #: HEN-010	Effective Date: April 4, 2012
Program: Hawai'i HIE	Revision Date: July 17, 2013
Approved By: Hawai'i HIE Board of Directors	

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, and to ensure that Authorized Users are adhering to Hawai'i HIE operational policies and procedures, and applicable state and federal laws.

Scope

This policy applies to the Hawai'i HIE and all Health eNet Participants, as well as their workforce members, business associates (BAs) and subcontractors. This policy pertains to the Health eNet Query only.

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.

Policy

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.

Audits of System Access by Users

Information Included in the Access Audit Log. The User access audit log shall 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;
- Identity of the patient whose information was accessed;
- Locations (i.e. IP addresses) that indicate via which network components an access event occurred;
- Type of information or record accessed (e.g. pharmacy data, laboratory data)
- **Whether the access was routine or a Break Glass event;**
- **Break Glass reason, if applicable; and**
- Source or location where the information is stored.

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 Participant's Site Administrator 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.

Access Audits by the Hawai'i HIE. The Hawai'i HIE will run ad hoc access audit reports for one or more Participants at least once every ninety (90) days, and work with those Participants to determine if any unauthorized activity has occurred.

Audits of Active Authorized Users

- On a periodic basis, at a minimum of once every ninety (90) days, 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.
- Participants and the Hawai'i HIE will review the reports and determine which, 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; and
 - Terminated, e.g. due to the User no longer being part of the Participant's workforce or disciplinary reasons;in the event appropriate changes to such Users' access authorities have not already been made by Site Administrators.
- Participants and the Hawai'i HIE will then follow the Modification of User Access and Leaves of Absence provisions of the Access Management policy.

Audits of Access Management

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. The Hawai'i HIE will review such audit logs on a periodic basis, at a minimum once every ninety (90) days.

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.

Release of Audit Reports to Individuals

A Participant shall provide an individual, upon request pursuant to the Individual Rights policy:

- A report containing Master Patient Index (MPI) information for the individual; or
- An accounting report listing disclosures of his/her protected health information.

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. At a minimum, the Hawai'i HIE's audit criteria will include:

- 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 Query participation statuses;
- Break Glass – Determine whether or not Users that accessed information through the Break Glass function went on to establish a patient relationship;

- Role-Based Authorizations – Determine which roles Site Administrators have designated for each Authorized User;
- Anomalous Patterns of User Activity – Anomalies may include excessive queries, excessive Break Glass 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.

Reports for anomalous patterns of user activity may include, but are not limited to:

- Break Glass Trending – Monitoring the number of times a User accessed records using Break Glass. The Hawai'i HIE may flag a User account if the Break Glass count exceeds established thresholds.
- Pediatric Specialty Practices – If a practice is listed as a pediatric specialty, the Hawai'i HIE monitors for Break Glass access when the patient is over the age of 18.
- Adult Special Practices – If a practice is listed as an adult specialty, the Hawai'i HIE monitors for Break Glass access when the patient is under the age of 18.
- 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 Break Glass access when the patient is a male.
- Geriatric Specialty Practices – If a practice is listed as a geriatric specialty, Hawai'i HIE monitors for Break Glass access when the patient is under the age of 50.
- Same Last Name – Monitoring for Break Glass access when Users and patients have the same last name.
- After Hours Access – Monitoring for any Break Glass events after regular business hours.

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.

The Participant and the Hawai'i HIE shall follow the provisions of the Incident Response and Mitigation policy to investigate the alleged unauthorized activity and take additional corrective actions if needed.

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.

Retention

Audit logs shall be retained for six (6) years.

Revision Rationale: Policy Review and Update	<input type="checkbox"/> New <input checked="" type="checkbox"/> Update <input type="checkbox"/> Consolidation
Date of Revision: July 17, 2013	Revision History:
Author(s), Title(s): Hawai'i HIE	