

TITLE: Access Management	
Policy #: HEN-005	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 describe the methods by which Authorized Users' access to the Hawai'i HIE Health eNet System will be provisioned, monitored and modified.

Scope

This policy pertains to access to the Health eNet by Users associated with valid Health eNet Participants. This policy applies to the Hawai'i HIE and all Health eNet Participants, as well as their workforce members, business associates and subcontractors.

Definitions

Authentication – The process for verifying that an individual, entity or software program accessing the Health eNet is the Authorized User the person, entity or program claims to be.

Authorization – The process of determining whether a particular User has the right to access the Health eNet, and determining the privileges associated with such access.

Authorized User, User – An individual who has met the requirements of this policy for obtaining Health eNet access authority.

Break Glass – A privilege that provides access to a patient's information in the Health eNet prior to the User establishing a treatment, payment or limited health care operations relationship with the patient.

Emergency – An overwhelming incident that exceeds the effective response capability of the impacted health care facility (e.g. another hospital needs to evacuate its patients, and this hospital must accommodate those incoming patients and staff to manage the emergency).

Provisioning – The process by which Authorized Users are granted authorization and access to use the Health eNet through an established unique user identity, password, and assignment of access rights and privileges based on the user's need to know/minimum access requirements.

Role-Based Access – The process for determining an Authorized User's Health eNet access rights and privileges based on the User's job function and the information needed to perform that job function.

Site Administrator – Individual responsible for performing duties, as directed by a Participant, related to activating and making changes to Authorized Users' Health eNet access privileges.

System Administrator – Hawai'i HIE workforce member responsible for performing duties related to maintenance of the Health eNet and support of the System's Authorized Users.

Very Important Person (VIP) – A status assigned to a patient by a Participant corresponding to additional or elevated security protocols (e.g. additional authentication and/or attestations of valid access by Users) applied to the patient’s record, based on the Participant’s policies and procedures.

Policy

Participants, the Hawai’i HIE, and their Authorized Users shall follow these requirements and standards when provisioning access to and using the Health eNet. Appendix A provides reference lists of Participants’ and Authorized Users’ key responsibilities under this policy.

Authentication Requirements and Controls

The Hawai’i HIE and Participants shall ensure that:

- The Health eNet User interface and access control systems for the System’s components; e.g. network, domains, servers, applications, database management systems, and workstations; utilize individual accounts with unique ID’s for each Authorized User;
- Any default User IDs installed with System-related software, devices or other components are removed, disabled or have had their passwords changed upon installation or initial logon;
- Authorized Users change their Health eNet passwords at least every ninety (90) days;
- Ensure that Health eNet passwords are a minimum of eight (8) characters in length, contain at least one capital letter, at least one number, and at least one special character;
- Ensure that Health eNet passwords are masked as they are typed by Users;
- Access to a Health eNet User account is locked after a maximum of five (5) consecutive unsuccessful attempts to login to the System;
- Restoration of access to a locked Health eNet User account requires the User to successfully answer at least one (1) security question or contact the Site Administrator to restore access to the User account; and
- The previous five (5) Health eNet passwords may not be used for the current password.

Authorized Users shall:

- Safeguard, and not share their User names and passwords used for accessing the Health eNet User interface and other System components with others;
- Not acquire or use the User names or passwords of other Health eNet Users or workforce members with access to System components; and
- Immediately notify the Site Administrator, and other system administrators as needed, if any passwords used to access the Health eNet or System components are compromised (i.e. acquired by someone other than the Authorized User), or cannot be reset by the User.

User Access Roles and Authorization

The Hawai’i HIE shall:

- Establish types of access roles that may be assigned to Authorized Users;
- Define the purposes for which Authorized Users in those roles may access protected health information (PHI) via the Health eNet;
- Define the types of information that Authorized Users within such roles may access (e.g., demographic data only, clinical data, User authority and privileges); and
- Determine which roles are provided special privileges to access PHI (e.g. Break Glass, VIP, confidential).

The Hawai’i HIE shall utilize the following role-based access standards to establish corresponding System

role types for Authorized Users. The Hawai'i HIE shall also define the purposes for which access may be granted and the types of information that may be accessed for each role type:

- Health eNet Query:
 - Practitioner (i.e. licensed health care provider) ED
 - Practitioner with access to clinical information, and Break Glass privileges
 - Non-practitioner with access to clinical information, and Break Glass privileges
 - Non-practitioner with access to clinical information, but no Break Glass privileges
 - Non-practitioner with access to non-clinical information
- Health eNet Secured Messaging:
 - Access to clinical information
 - Access to non-clinical information
- Health eNet Site and System Administration:
 - Health eNet System Administrator with access to non-clinical information
 - Health eNet System Administrator with access to clinical information to fulfill requirements of the Hawai'i HIE's operational policies and applicable laws

User Awareness and Training

Each Participant and the Hawai'i HIE are responsible for training and ongoing supervision of their Authorized Users to ensure awareness of and compliance with HIPAA, other applicable laws and Hawai'i HIE operational policies and procedures. Each Participant shall also train and supervise its Authorized Users regarding any of the Participant's policies and procedures that pertain to the Health eNet. Such training shall be provided to each new Authorized User prior to activation of his/her Health eNet User account, and annually thereafter.

Provisioning of User Access

Participants. Each Participant shall designate Health eNet Authorized Users from among its workforce. A Participant shall assign an access role to each User, based at a minimum on the User's job function and relationship to patients of the Participant. The Participant's Site Administrator shall activate each new User's access, in accordance with the role assigned by the Participant.

Hawai'i HIE. The Hawai'i HIE shall designate Health eNet System Administrators from among its workforce. The Hawai'i HIE shall assign an access role to each System Administrator, based at a minimum on the System Administrator's job function related to System maintenance and audit, and support of Authorized Users. The Hawai'i HIE's IT Manager shall activate each new Site Administrator's access, in accordance with the role assigned by the Hawai'i HIE.

Monitoring of User Access

The Hawai'i HIE shall actively monitor use of the Health eNet, based on the provisions of its Audit policy.

Reports of Active Users. The Hawai'i HIE shall periodically run audit reports listing the current active Authorized Users and their respective Health eNet access roles for each Participant. The Hawai'i HIE shall then provide the reports to the Participants for review to determine if modifications to any Users' access authorities, based on changes to job responsibilities or employment status, are required.

Reports of User Access Activity. The Hawai'i HIE shall periodically run audit reports of Participants' and its own Users' activity to identify potential instances of unauthorized access, use or disclosure of information via the Health eNet.

HEN-005

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 the Participant that contributed the information to the System.

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.

Modification of User Access

In the event of a change in job responsibilities or employment status of an Authorized User, or confirmation that a User is responsible for unauthorized access, use or disclosure of information via the Health eNet:

- Participant User. A Participant shall, as necessary, direct the Site Administrator to modify, suspend or terminate the User's Health eNet access authority.
- Hawai'i HIE User. The Hawai'i HIE shall, as necessary, direct a System Administrator to modify, suspend or terminate the User's Health eNet access authority.

Modifications of User access shall be made prior to, during or immediately following a change in job responsibilities or employment status, or detection of unauthorized System activity, to prevent unauthorized access or use of the System.

Inactive Accounts. The Hawai'i HIE will suspend a Health eNet Authorized User account that is inactive for at least ninety (90) consecutive days. The Hawai'i HIE will notify the Participant associated with the User prior to suspending the account to determine if the account should remain active. If an account remains inactive for one (1) year, the account will be deactivated.

Leaves of Absence. A Participant may direct its Site Administrator to suspend the access authority of a User who will be on a sabbatical or other voluntary long-term or indefinite leave of absence.

Transfer of Access to Patient Records Between Participants

In the event a Participant intends to completely transfer its accountability for patient records to another provider, e.g. due to closure of a practice or business, the Participant will notify the Hawai'i HIE at least thirty (30) days in advance of the transfer, or as soon as possible if the decision to make the transfer is less than thirty (30) days from the scheduled transfer date or the transfer has already occurred.

The Hawai'i HIE may terminate the User accounts associated with the Participant once the Participant has provided confirmation that the transfer is complete, or the Hawai'i HIE determines that the transfer is complete. Otherwise, such User accounts will be suspended and deactivated in the same manner as other inactive accounts.

The Participant making the transfer will provide the name and contact information of the party to whom the patient records will be or have been transferred. The Hawai'i HIE will determine if the party assuming accountability of the records is a Health eNet Participant, and if so the Hawai'i HIE may facilitate transfer of access to the patients' information in the System from one Participant to the other.

Emergency Access and Use

The Hawai'i HIE will configure the Health eNet Query to provide, in the event of an emergency situation or disaster: 1) access authority for a new Authorized User to temporarily access the System, and 2) a temporary increase of access authority (e.g. privilege to Break Glass) for an existing User. Site Administrators may activate or modify Authorized Users' accounts to include such capabilities only in response to emergency or disaster situations, as directed by their Participating Organizations.

Internal Hospital Use. Administrators for a hospital that is a Health eNet Participant may declare an emergency situation for their facility. The Site Administrator will follow the Participating Organization's policies and procedures for providing access and increasing access privileges in an emergency situation.

External Disasters. A disaster condition is determined by the Governor of the State of Hawai'i. In the event of a disaster, Health eNet Participants may assume that each affected hospital's emergency management plans have been fully implemented. Site Administrators will follow their Participating Organizations' policies and procedures for providing access and increasing access privileges in a disaster situation.

Retention of User Accounts and User Account History

The Hawai'i HIE will secure terminated or otherwise deactivated Health eNet User accounts, and record access to such accounts, to safeguard against their unauthorized access or use.

The Hawai'i HIE will record and maintain an historical log of all active and inactive User accounts for audit and investigative purposes.

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

Appendix A

Participants' Key Responsibilities

Each Participant has the responsibility to:

- Designate a Site Administrator. The Site Administrator may be the same individual as the Participant's Operations Management Point of Contact (OMPOC) or the Hawai'i HIE, as described in the Participation Requirements policy.
- Designate Health eNet Authorized Users from among its workforce;
- Assign an access role to each Authorized User;
- Provide initial and annual training to its Authorized Users regarding HIPAA, other applicable laws and policies and procedures pertaining to the Health eNet.
- Supervise its Authorized Users to meet the requirements of such laws, policies and procedures, and holding its Users accountable for doing so;
- Direct the Site Administrator to activate, terminate, suspend or modify access authorities of Users as necessary;
- Notify the Hawai'i HIE of events that may involve unauthorized access, use or disclosure of information via the System; and
- Identify business associates (BAs) and subcontractors with valid purposes for participating in the Health eNet on behalf of the Participant. Such BAs and subcontractors, upon meeting the Health eNet participation requirements of the Hawai'i HIE's operational policies, may in turn establish Health eNet access for their Authorized Users by following the provisions of this policy.

Authorized Users' Key Responsibilities

Prior to accessing the Health eNet, each Authorized User must:

- Complete and Sign an Authorized User Application Form – The signed form serves as the User's access request, and agreement to abide by policies and procedures, confidentiality requirements and other terms and conditions of using the Health eNet; and
- Complete training, as required by this policy.

Upon being provisioned access to the Health eNet, each Authorized User must:

- Limit use of the System to the activities permitted for the User's job function on behalf of the Hawai'i HIE or Participant, even if his/her user role permits activities beyond the scope of duties within that job function;
- Limit access, use and disclosure of information via the System to the degree and duration of time necessary to perform a given authorized task (e.g. for patient care, System administration, fulfilling a request for access, amendment or accounting of disclosures of PHI);
- Report any potential unauthorized access, use or disclosure of information via the Health eNet, or any attempt to tamper with the System, to an appropriate point of contact responsible for receiving notifications of such events within his/her Participating Organization;
- Not share his/her user names or passwords used for accessing the Health eNet user interface or other System components with others; and
- Not acquire or use the user names or passwords of other Health eNet Users or workforce members with access to System components; and
- Immediately notify the Site Administrator, and other system administrators as needed, if any user names or passwords used to access the Health eNet or System components are forgotten or compromised, or need to be reset.