HEALTH INFORMATION TECHNOLOGY EXCHANGE OF CONNECTICUT

POLICY AND PROCEDURE

Policy Name/Subject: HITE-CT AUTHENTICATION POLICY V1.0	Policy Number: 3	Approved By: HITE-CT Board
Approval Date: 11-21-2011	Effective Date: 11-21-2011	Revision Date(s): 11-21-2011

PURPOSE: The purpose of the policy is to ensure that systems and persons interacting with the HITE-CT system are known through the process of reliable security identification of subjects by incorporating an identifier and its authenticator.

DEFINITIONS:

Audit Trails and Node Authentication (ATNA)
IHE profile that specifies technical requirements supporting audit.

Business Associate

(A) An individual or entity who, on behalf of a covered entity or of an organized health care arrangement (as defined pursuant to 45 CFR 164.501) the covered entity participates in, excluding a member of the covered entity's workforce, performs, or assists in the performance of:

a. A function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
b. Any other function or activity regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); or

(B) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, or to or for an organized health care arrangement, where the provision of the service involves the disclosure of PHI from the covered entity or arrangement, or from another business associate of the covered entity or arrangement, to the individual or entity.

A covered entity may be a business associate of another covered entity. [45 CFR 160.103]

Data Use and Reciprocal Support Agreement (DURSA)
A comprehensive agreement that governs the exchange of health data between participants in HITE-CT.

Health Information Technology Exchange of Connecticut (HITE-CT)
A quasi-public agency of the State of Connecticut charged by statute with promoting, planning and designing, developing, assisting, acquiring, constructing, maintaining and equipping, reconstructing and improving healthcare information technology, including the electronic exchange of health information . Also, HITE-CT is a business associate of all participating members pursuant to the HITECH Act.

HITE-CT Infrastructure Service Provider

The entity operating and managing the core services supporting the HITE-CT systems (e.g. Provider Registry, Patient Identity Cross Reference Index Manager, Audit Record Repository, Document Registry, Document Repository, etc.).

Individually Identifiable Health Information
Information that is a subset of health information including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearing house; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 CFR 160.103.

May
Permits the action to happen, but does not require it.

Participating Health Care Subscriber (PHCS)
Any healthcare provider that has executed an effective Data Use and Reciprocal Support Agreement (DURSA) with HITE-CT. See Member List (www.hitect.org/members).

Protected Health Information (PHI)
Individually identifiable personal information in any form or medium about the past, present or future physical or mental health or condition of an individual, or the past, present or future payment for the provision of healthcare to an individual, [pursuant to federal and state law]. 45 CFR 160.103

Shall
The action must be taken.

Should
It is a recommendation that an action ought to be done, but it is not required.

SCOPE/APPLICABILITY:

This policy applies to HITE-CT, to all persons and organizations that have access to HITE-CT managed health records, including those connected to the HITE-CT (PHCSs), their Business Associates, as well as any subcontractors of Business Associates that perform functions or provide services involving the use and disclosure of PHI, the HITE-CT Infrastructure Service Provider, and any other subcontractors of HITE-CT. This policy applies to all Protected Health Information (PHI) provided to or retrieved from the HITE-CT systems.

POLICY:

- EHR products or modules must have successfully completed NIST defined Meaningful Use Authentication Testing conducted by ONC approved or ANSI Accredited Certification Bodies. Products or modules that have not yet completed this testing will be considered on a case-by-case basis.
- EHR products or modules must have successfully completed NIST defined Meaningful Use Emergency Access Testing conducted by ONC approved or ANSI Accredited Certification

Bodies. Products or modules that have not yet completed this testing will be considered on a case-by-case basis.

- EHR products or modules must have successfully completed NIST defined Meaningful Use Automatic Logoff Testing conducted by ONC approved or ANSI Accredited Certification Bodies. Products or modules that have not yet completed this testing will be considered on a case-by-case basis.
- All HITE-CT remote access SHALL require strong authentication (multi-factor authentication).
- All HIE Nodes exchanging PHI SHALL implement the IHE Audit Trails and Node Authentication (ATNA) as specified by the IHE IT Infrastructure Technical Framework(IHE ITI TF-2a: 3.20 Record Audit Event) logging requirements as amended from time-to-time.
- PHCSs should also assert strong authentication to their remote access and require the use of appropriate authentication methods for users of the HITE-CT systems.
- A directory of provider data sources and data consumers within the HITE-CT will include primary contact information of registered members, identity attributes of providers, organizations and systems. The primary contact information for the data in the directories supplied to the directory should include primary contact name and any contact phone numbers.
    - For Connecticut licensed practitioners and healthcare organizations, this information SHALL be sourced through the Connecticut practitioner and healthcare organization license databases.
    - For non-licensed practice locations, this information SHALL be sourced the information gathered upon connecting the organization to HITE-CT systems.
    - For employees and staff of healthcare and supporting organizations, this information SHALL be provided by the designated contact within the PHCS.
    - Notification of terminations of employees or modification of provider privileges (e.g. license status) SHALL be updated in the user directory within one business day of notification to HITE-CT.
    - PHCSs SHALL notify HITE-CT at the time of termination of affiliation of an individual from the organization.
- The HITE-CT will collect the attributes as needed for unique identification of the individual accessing the information in the HITE-CT[1]. Required elements are profession, role, name, the practice address (not home address), identity service provider and organization affiliation, business/legal address and License/ID. Other attributes that are required, if they exist for this individual, includes:
    - Specialization/ specialty,
    - Email address,
    - National Provider Identifier (NPI), and
    - Digital identity.
- Identifying the organization requires collecting the following attributes: organization name and email address. Other attributes are required if they exist, including:
    - Digital identity,
    - EDI administrative contact,

[1] 45 C.F.R. § 164.312(a)(2)(i) (requiring assignment of a unique name or number for identifying and tracking user identity).

  - Clinical information contact,
  - Service Location, and
  - Predecessor name and date of change.
- If the HITE-CT is a regulated healthcare organization, all supporting organization attributes above are required, as well as:
  - License/ID,
  - License status,
  - Registered name, and
  - Registered address.
- Identifying the system requires the attributes of:
  - System name,
  - Digital identity,
  - Organization affiliation,
  - System IP address, and
  - System domain name.
    - If there is no system domain name, the system IP address may be used. For purposes of identifying the originating electronic data sources, would require a date stamp and at least one of the following is required: the system (1) name, (2) IP address, or (3) domain name. Any identifying system types, such as the laboratory information systems, electronic health record system, emergency medical system, etc should also be included.
- Proper registration requires the establishment of a defined role associated with the registered user.
  - The individual's organization role[2] is required for role based access and should include the context of the organization. If the healthcare functional role[3] or the structural roles[4] exists, they are also required.
- Identity is verified through authentication of the user, the organization and the HITE-CT's system.[5]
- The methods for user identity vetting include both verifying the identity in person by a trusted authority and verification through the use of a demonstrated government-issued ID. The trusted authority is recognized by the state or federal government.
- An applicant requesting an identity tied to a regulated provider type must have provider licensure validation. It is acceptable that this occur along with the validation required of any employee of a licensed provider organization. Also, the HITE-CT use of a specific naming convention as a primary identifier is required with a minimum assurance level used of Medium (knowledge/strong password/shared secret).

[2] As defined in the American Health Information Community (AHIC) Use Cases.

[3] The functional role is dynamic and is a function of the role in which you are acting.

[4] A structural role is persistent and can be mapped to professions that are recognized.

[5] 45 C.F.R. § 164.312(d) (requiring "procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed").

- Organization identity vetting can be accomplished through personal knowledge of a registration authority, that the organization is who they say they are by a demonstrated documentation of corporate existence. The HITE-CT is required to use a specific naming convention as a primary identifier, and this would include the use of object identifier (OID) or idiosyncratic naming, if either of these exists. This is a requirement at the state level and the ASP Collaborative recommends development of a naming convention that can be registered and identified nationally.
- The minimum assurance level required for organization authentication is High (PKI/Digital ID).
- System identity vetting, ensuring the data are coming from the system that they are supposed to be coming from, requires the assertion by an authorized organization representative and/or the demonstration of association with another licensed organization.
- The user identity, role and affiliation must be checked for both revocation and expiration at the time of logon to the system. If either case pertains, use would be denied.

  The HITE-CT is responsible for digital verification of non-repudiation signer credentials. Verification implies that:
  - The credential issued by a trusted authority,
  - The credential is current,
  - The credential is not suspended or revoked, and
  - The credential type is appropriate (for example, physician or pharmacist).

  If the signed-by-person claimed (non-repudiation) exists, it should also be verified.
- It is required that the level of assurance be declared and should be communicated in terms of the then current National Institute of Testing and Standards (NIST) requirements. For the HITE-CT to migrate data an assurance level of at least Medium (knowledge/strong password/shared secret) is required.
- If the HITE-CT is exchanging for purposes of treatment, the provider seeking access needs to be able to demonstrate or certify that they have a treatment relationship with the patient. Note that this does not need to be asserted at each access.
- The HITE-CT is required to have the ability to use digital signatures, if they exist, at least at the provider level.
- The use of persistence[6] of the source signature is required and is the responsibility of the HITE-CT with its own participants. The attributes required are persistent user signature, persistent organization signature and persistent system signature. Non-repudiation of origin is also the responsibility of the HITE-CT with its own participants, and includes the attributes of user, organization and system accountability. If source authentication exists it is also required.
- The transmission of caveats regarding data completeness is required to indicate that an entire record may not have been transmitted. The use of pertinent state-specific caveats should be included in the transmission.
- The identity of the recipient must be established and the method of identifying recipients of communications can include, but is not restricted to: (1) derived from ordering system communications, (2) selected from a provider directory, or (3) derived from identifiers included in the request for information.

[6] Persistence indicates proof that data has not been altered and is only valid during the communication session.

- For the purposes of cross-HIE verification, the ability to use digital signatures is required at the provider level.

  The use of persistence of the source signature is required and is the responsibility of the HITE-CT with its own participants. The attributes required are:

  - Persistent user signature,
  - Persistent organization signature and,
  - Persistent system signature.

  Non-repudiation of origin is also the responsibility of the HITE-CT with its own participants, and includes the attributes of:

  - User Accountability,
  - Organization Accountability, and
  - System accountability.

  If source authentication exists, it is also required.
- For purposes of data authentication, the use of a timestamp is required at point of signature application.
- Data validation of signer credentials should be issued by a trusted authority should be current, and the credential should not be suspended or revoked, and the credential type should be appropriate (for example, physician, pharmacist or hospital). For purposes of data integrity, the data validation should indicate that the data has not been changed since the signature, and should have a timestamp at point of signature application.
- For verification purposes the requestor type should identify the exchange, organization (institution) and the user (individual).
- The signature purpose should be included as a minimum requirement, and any of the captured signature elements that exist should be included.

PROCEDURE:

Policy Maintenance

The Legal and Policy Committee is responsible for monitoring and maintenance of policies.