HEALTH INFORMATION TECHNOLOGY EXCHANGE OF CONNECTICUT

POLICY AND PROCEDURE

Policy Name/Subject: HITE-CT IDENTITY MANAGEMENT POLICY V1.0	Policy Number: 2	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 the identities of the persons and entities interacting with HITE-CT are assured through the performance of tests to enable a data processing system to recognize entities (individuals or machines interacting with the HITE-CT system).

DEFINITIONS:

Applicant

A party undergoing the processes of registration and identity proofing to enable access to HITE-CT system user interfaces (e.g. Patient/consumer, employees of health institutions, Regulated Health Professional, healthcare institutions)

Assurance

In the context of NIST SP 800-63, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. (NIST 800-63-1)

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]

Certification Authority (CA)

A trusted entity that issues and revokes public key certificates.

Certificate Revocation List (CRL)

A list of revoked public key certificates created and digitally signed by a Certification Authority. (NIST 800-63-1)

Credential

An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. (NIST 800-63-1)

Healthcare Consumer
(Individual)

Person that is the receiver of health related services and that is a person in a health information system. Any person who uses or is a potential user of a health care service, subjects of care may also be referred to as patients, health care consumers or subject of cares. [ISO TS22220]. In the US, this may be referenced as an 'individual', which means the person who is the subject of protected health information.

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.)

Healthcare Organization

(Covered entity)

Officially registered organization that has a main activity related to health care services or health promotion. [ISO IS17090]. In the US, the Healthcare Organization is known as a 'Covered entity':

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

Identification

Performance of tests to enable a data processing system to recognize entities. [ISO/IEC 2382-8:1998]

Identifier

Piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator. [ENV 13608-1]

Identity
A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique. [NIST 800-63-1]

Identity Proofing
The process by which a Certificate Services Provider (CSP) and a Registration Authority (RA) validate sufficient information to uniquely identify a person. [NIST 800-63-1]

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.

Non-Regulated Health Professional
Person employed by a health care organization who is not a regulated health professional.
EXAMPLES: Medical receptionist who organizes appointments or a nurse's aid who assists with patient care.
NOTE: The fact that a body independent of the employer does not authorize the employee's professional capacity does not, of course, imply that the employee is not professional in conducting her/his services. [ISO IS17090]

Organization Employee
(Workforce member)
Person employed by a health care organization or a supporting organization.

EXAMPLES: Medical records transcriptionists, health care insurance claims adjudicator, and pharmaceutical order entry clerks. [ISO IS17090]

In the US, this may be referred to as 'Workforce member': employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Organization Roles
Organizational roles correspond to the hierarchical organization in a company in terms of internal structures. [Neumann/Strembeck]

Participating Health Care Subscriber (PHCS)

Any healthcare institution or healthcare professional, which 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

Registration Authority (RA)
A trusted entity that establishes and vouches for the identity of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s). [NIST 800-63-1]

Regulated Health Professional
(Practitioner) Person who is authorized by a nationally recognized body and qualified to perform certain health services. [ISO 17090]. In the US, this is referred to as a Health care provider: a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

EXAMPLES: Physicians, registered nurses, and pharmacists.
NOTE 1: The types of registering or accrediting bodies differ in different countries and for different professions. Nationally recognized bodies include local or regional governmental agencies, independent professional associations, and other formally and nationally recognized organizations. They MAY be exclusive or non-exclusive in their territory.
NOTE 2: A nationally recognized body in this definition does not imply one nationally controlled system of professional registration but, in order to facilitate international communication, it would be preferable for one nationwide directory of recognized health professional registration bodies to exist

Role
Set of competences and/or performances that are associated with a task. [ISO TS21298]

Secure Node
The secure node is responsible for providing reasonable access controls. This typically includes user authentication and authorization. The secure node is also responsible for providing security audit logging to track security events. The difference between the Secure Node and the Secure Application is the extent to which the underlying operating system and other environment are secured. A Secure Node includes all aspects of user authentication, file system protections, and operating environment security. The Secure Application is a product that does not include the operating environment. [IHE Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 64)]

Shall

The action must be taken.

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

Sponsored Health Care Provider
Health services provider who is not a regulated professional in the jurisdiction of his/her practice, but who is active in his/her health care community and sponsored by a regulated health care organization

EXAMPLES: A drug and alcohol education officer who is working with a particular ethnic group, or a health care aid worker in a developing country. [ISO IS17090]

Subscriber
A party who receives a credential or token from a CSP. [NIST 800-63-1]

Supporting Organization
Officially registered organization which is providing services to a health care organization, but which is not providing health care services.

EXAMPLES: Health care financing bodies such as insurance institutions, suppliers of pharmaceuticals and other goods. [ISO IS17090]

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 HITE-CT systems.

POLICY:

- Organization systems connecting to HITE-CT systems SHALL be subject to Trusted Third Party Attestation for the issuance of organization system digital certificates
- Digital certificates used for authentication or digital signatures SHALL be issued by a Certification Authority that is Federal Public Key Infrastructure (PKI) Bridge Certified
- The Certification Authority SHALL support conformance to ISO IS17090 Health Informatics – Public Key Infrastructure
- Identity proofing requirements for individuals areas follows:
    - Identity proofing for all individual certificates SHALL require a government issued photographic identification or ID (i.e. passport, driver's license, military ID, state/federal ID, A I551 Alien Registration Card, foreign government issued ID) for identified Healthcare consumer (anonymous Healthcare consumers need not provide verification).
    - Identity proofing for regulated healthcare providers SHALL require evidence of a current License issued by the appropriate licensing agency
        - Practitioners, Healthcare provider organizations: Department of Public Health Practitioner Licensing and Investigations Section

- Pharmacists, Pharmacies, and Pharmacy support professions: Drug Control Division of the Department of Consumer Protection
- Insurance companies: State of Connecticut Insurance Department
- Non-Healthcare organization trading partners and supporting organizations: Connecticut Secretary of State

- Identity proofing for all individual certificates SHALL include a face-to-face attestation of the individual's identity.
- Identity proofing for healthcare employees SHALL require verification of employee ID or letter from employer on employer letterhead indicating current employment status.
- Identity proofing of a sponsored healthcare provider SHALL require a letter from a regulated health care professional or authorized representative of a sponsoring regulated health organization to establish that they are active in their health care community.

- Identity proofing requirements for organization systems are as follows:
  - Identity proofing of an Organization's Secure Node SHALL require attestation by an individual identified by the organization as authorized to provide such attestation.
    - A letter on the entity letterhead signed by a corporate officer. , This letter shall identify a representative of the entity authorized to validate and request organization or device certificates on behalf of the entity.
  - The organization responsible for the system shall provide proof of a current license to conduct the healthcare or healthcare associated business and one of the following:
    - tax exemption certificate, or
    - tax ID number, or
    - DEA number, or
    - NPI number, or
    - A copy of the Articles of Incorporation, or
    - A current Dunn and Bradstreet Report, or
    - A Certificate of Good Standing from the state.
  - A current health care license issued in accordance with Connecticut State law.
- Electronic identity credentials SHALL NOT be issued until a subscriber agreement addressing the credential holder's requirements is completed and signed.
- Procedures for account revocation upon employee severance and notifications for HITE-CT system account revocations SHALL be implemented by any organization for any employee that has been issued an individual identity credential to access HITE-CT systems as an Organization Employee.
- The Registration Authority will verify the documents presented by the Applicant for registration and identity proofing are as designated in the documentation requirements section above.
  - ISO Individual Identity types listed above will be issued under the following Federal Bridge policy designations:

    - Patient/Healthcare consumer – Affiliated or unaffiliated as described below.
    - Supporting Organization Employee – Affiliation is with the employer.
    - Sponsored Health Care Provider – Affiliation is with the sponsor.
    - Regulated Health Professional – Affiliation is with the Department of Public

Health (DPH) Practitioner Licensing and Investigations Section as described below.

  - Non-Regulated Health Professional – Affiliation is with the employer

- Regulated Health Professional: For regulated health care practitioners, an affiliated identity shall be issued such that the designated affiliation is either "DPH Practitioner Licensing or Investigations Section" or a regulated health care provider organization. Where the regulated health professional is a pharmacist, pharmacy intern, or pharmacy technician, the designated affiliation is either "CT Department of Consumer Protection" or a regulated pharmacy, drug manufacturer, or drug distributor. The CT-HISPI authorized Local Registration Authority will notarize the application and subscriber agreement.
  - The Local Registration Authority will verify the current license status with the DPH Practitioner Licensure and Investigations section prior to authorizing the issuance of a regulated health care professional identity.
  - The Local Registration Authority will verify the current license status with the CT Department of Consumer Protection prior to authorizing the issuance of a regulated health care professional identity for pharmacists, pharmacy interns, or pharmacy technicians.

- Employer Responsibility: Employers with employees/staff issued digital identities for use within CT-HISPI, shall notify a CT-HISPI authorized Local Registration Authority when an employee/staff has separated from a participating organization or when the employee/staff has had a change in responsibility concerning their role assigned as part of the certificate issuance process. Where the separation is an individual authorized to assign organization or device credentials on behalf of the organization, a replacement designee for assignment of these credentials shall follow this notification
- Subscribers shall notify a CT-HISPI authorized Local Registration Authority if their digital identity is lost, stolen, or otherwise known to be compromised. This will result in a revocation request and request for a new digital certificate.
- Account subscriber agreements SHALL include the requirement to protect the subscriber identity credential

Policy Maintenance

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