HEALTH INFORMATION TECHNOLOGY EXCHANGE

OF CONNECTICUT

POLICY AND PROCEDURE

Policy Name/Subject:	Policy Number:	Approved By: HITE-CT Board
HITE-CT INFORMATION SECURITY POLICY V1.0	9	
Approval Date: 11-21-2011	Effective Date: 11-21-2011	Revision Date(s): 11-21-2011

PURPOSE:

The purpose of the policy is to reasonably ensure that information security is conducted in a manner that protects individually identifiable health information that comprises protected health information (PHI) as defined pursuant to 45 CFR 160.103 and that supports the availability, confidentiality, integrity, and accountability of HITE-CT shared clinical information.

DEFINITIONS:

Access Control

A means of reasonably ensuring that the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource of a data processing system, facility or other such storage of PHI can be accessed only by authorized entities in authorized ways. [45 CFR 164.304, 164.308, 164.310]

Accountability

Property ensures that the actions of an entity may be traced to that entity. [ISO 7498-2:1989]

Availability

The property that data or information is accessible and useable upon demand by an authorized person. [45 CFR 164.304]

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]

Confidentiality

The property that data or information is not made available or disclosed to unauthorized persons or processes. [45 CFR 164.304]

Data Integrity

The property that data or information have not been altered or destroyed in an unauthorized manner.. [45 CFR 164.304]

Data Origin Authentication

Corroboration that the source of data received is as claimed. [ISO 7498-2:1989]

De-identification

Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information. [45 CFR 164.514(a)].

May

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

Node Authentication

Node Authentication - Describes authenticating each computer system in a network that can host one or more databases. [Each node in a distributed database system can act as a client, a server, or both, depending on the situation.]

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.

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

Security or Security Measures
All of the administrative, physical, and technical safeguards in an information system. This includes protecting the availability, confidentiality, integrity, and accountability of data and related assets. [ENV 13608-1, 45 CFR 164.304]

Shall
The action must be taken.

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

Trading Partners
Entities that exchange (submit or receive) data electronically with each other. Examples include any pairing of physicians, providers, billing services, clearinghouses, health plans or third-party administrators.

SCOPE/APPLICABILITY:

This policy applies to HITE-CT, the HITE-CT (PHCSs), 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:

- Systems storing data required for the operations and functionality of HITE-CT SHALL be managed in accordance with 45 CFR 164 Subpart B. Such systems include:
    - Patient Identity Resolution Services
    - Document Registries
    - Document Repositories
    - Audit Record Repositories
    - Provider Directories
    - HITE-CT Portal

    - HITE-CT Infrastructure Transformation Services
- Systems storing data required for the operations and functionality of HITE-CT SHOULD be managed in accordance with ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002.
- Participating HCSs and Participating Users providing or retrieving PHI from the HITE-CT systems and operating systems storing data required for the operations and functionality of HITE-CT SHALL implement policies and protections for Access Control, Automatic Logoff, Audit Log, Emergency Access, Integrity, Authentication, General Encryption, Encryption when Exchanging Electronic Health Information and other administrative and physical safeguards as defined in the HIPAA Security Rule. [45 CFR 164 Subpart B]
- All HITE-CT Infrastructure Service components (Patient Identity Cross Reference Index Manager, Document Registry, Document Repository, Audit Record repository, Provider Directory, eAuthentication services etc.) SHALL be managed in an environment conforming to one of: ENHAC (infrastructure), SAS70 or SSAE 16 (nodes), and as defined in the HIPAA Security Rule supporting physical safeguards, clearance, access, supervising those with access and other core secure management practices.
- All HITE-CT Infrastructure Service components SHALL implement contingency and disaster recovery to assure availability of HITE-CT managed health information.
- All HITE-CT Infrastructure Service components SHALL conform to the capabilities as required for Meaningful Use 45 CFR Section 170.302(u) General Encryption.
- All HITE-CT Infrastructure Service components SHALL conform to the capabilities as required for Meaningful Use 45 CFR Section 170.302 170.302(v) Encryption when Exchanging Electronic Health Information.
- All HITE-CT Infrastructure Service components SHALL Encrypt PHI at Rest.
- All HITE-CT Infrastructure Service Business Associates shall comply with the HIPAA Security Rule and the use and disclosure provisions of the HIPAA Privacy Rule pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act, as may be amended from time to time. [45 CFR 164 Subpart B and Subpart E]
- All HITE-CT Infrastructure Service components SHALL implement Intrusion Detection or Prevention measures.
- PHCSs shall comply with any and all requirements of the HIPAA Security and Privacy Rules (45 CFR 164 Parts C & E) including, but not limited to, the establishment of necessary Security Measures, protections around the use and disclosure of PHI, required personnel training, and sanctions for inappropriate use of HITE-CT managed information and services.

- Participating HCSs SHALL have contingency plans in place for extended downtime periods to continue operations in the absence of HITE-CT services.

Policy Maintenance

The Legal and Policy Committee is responsible for monitoring policy maintenance.