HEALTH INFORMATION TECHNOLOGY EXCHANGE OF CONNECTICUT

POLICY AND PROCEDURE

Policy Name/Subject: HITE-CT PRIVACY AND SECURITY AUDIT POLICY V1.0	Policy Number: 1	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 the security and confidentiality of patient data within the HITE-CT systems through both internal and external audits.

DEFINITIONS:

Audit

Systematic and independent examination of accesses, additions, or alterations to electronic health records to determine whether the activities were conducted, and the data were collected, used, retained or disclosed according to organizational standard operating procedures, policies, good clinical practice, and applicable regulatory requirement(s).

Audit Log

Chronological sequence of audit records, each of which contains data about a specific event.

Audit Record

A record of a single specific event in the life cycle of an electronic health record.

Audit Record Repository (ARR)

Receives and stores audit records from sources and consumer of the HITE-CT managed health information.

Audit Trail

Collection of Audit Records from one or more Audit Logs relating to a specific Healthcare Consumer or a specific electronic health record.

Audit Trails and Node Authentication (ATNA)

IHE profile that specifies technical requirements supporting audit.

Breach

The acquisition, access, use, or disclosure of Unsecured PHI in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of the PHI. To compromise the security or privacy of PHI means to pose a significant risk of financial, reputational or other harm to the individual whose PHI is involved. Breach excludes (i) any unintentional acquisition, access, or use of PHI by a Workforce Member or person acting under the authority of a Covered Entity (PHCS) or a Business Associate, if such acquisition, access, or use was made in good faith and with the scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule, (ii) any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity (PHCS) or Business Associate to another person authorized to access PHI at the same Covered Entity (PHCS) or Business Associate, or Organized Health Care Arrangement in which the Covered Entity

(PHCS) participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule, or (iii) a disclosure of PHI where a Covered Entity (PHCS) or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. All Breaches are Reportable Events, however, not all Reportable Events are Breaches.

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.

External Privacy and Security Audit

Review by an independent third party to ensure that the systems being audited are managed according to specified requirements.

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.

Health Information Technology Exchange of Connecticut Health Information Exchange (HITE-CT)
The health information exchange network operated by HITE-CT.

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.).

Health Information Exchange Nodes (HIE Nodes)
HIE nodes are those systems (Electronic Medical Records, Public Health Information Systems, Infrastructure systems) that are connected to HITE-CT systems.

Identifier
ID
A character or group of characters constituting a value which is used to distinguish one entity from another. (Adapted from ISO 6523.) For the purposes of Audit, Identifiers are used to indicate:

- Document Unique ID: An unique Identifier assigned to a document, including medical summary documents and other HITE-CT managed documents
- User ID: the identity of the user that is logged in to the session that initiates an audit log
- Person ID: the identifier associated with a person that is requesting or receiving a disclosure
- System ID: the identifier associated with the machine or system requesting or receiving a disclosure
- Consent or Authorization ID: the identifier associated with the document that is recorded that allows for the disclosure of information.

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.

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.

Internal Privacy and Security Audit
Review by HITE-CT or HITE-CT service providers to ensure that the systems being audited are managed according to specified requirements.

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).

Privacy and Security Audit
Audit focused on assuring conformance to privacy and security practices and procedures.

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

Reportable Event
An action (or lack of action) that violates HITE-CT policies and procedures for accessing or using protected health information managed by the HITE-CT systems. Such violations may be unintentional or intentional.

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:

- All persons or entities to whom this privacy and security audit Policy applies, as well as their Business Associates must implement technical processes that accurately record activity related to access, creation, modification and deletion of electronic PHI.
    - EHR products or modules must have successfully completed NIST defined Meaningful Use Audit Log 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 are recommended to have successfully completed NIST defined Meaningful Use Accounting of Disclosures Testing conducted by ONC approved or ANSI Accredited Certification Bodies. (NOTE: Optional MU test for EHRs)
    - 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.

- As a part of log-in monitoring, an Audit Log is required to be created to record when a person logs on to the network or a software application of the HITE-CT. This includes all attempted and failed logons.
- An additional Audit Log should be captured by the HITE-CT systems for a subset of the subject identity attributes that have been used when a person is found.
- The HITE-CT Privacy and Security Audit Logs shall include:
  - User ID,
  - A date/time stamp,
  - Identification of all data transmitted (document unique ID), and
  - Authorization Document with unique ID for a authorizations published
- For purposes of information disclosure, Privacy and Security Audit SHALL include documentation of the following :
  - The date and time of the request,
  - The reason for the request,
  - A description of the information requested, including the data accessed, the data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to another party,
  - The Identifier of person/system requesting disclosure,
  - The Identifier /verification of the party receiving the information,
  - The Identifier of the party disclosing the information.
  - A registration of a consent document SHALL include the consent/authorization Identifier.
- For purposes of information requests, a written policy is required that includes the following components:
  - The date and time of the request,
  - The reason for the request,
  - A description of information requested, including the data accessed, data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to, or printed by another party,
  - The Identifier of person/system requesting disclosure,
  - The Identifier /verification of the party receiving the information,
  - The Identifier of the party disclosing the information,
  - The method used for verification of the requesting entity's identity.

- HITE-CT systems SHALL generate Audit Logs that are required to record activity specified by HITE-CT and the HITE-CT Privacy and Security Officer shall periodically review the generated Audit Logs, at least quarterly. This review of the Audit Logs is based on established audit criteria and shall include documentation of any anomalies. HITE-CT will document its mitigating action (including sanctions, security incident response team activation, etc. as appropriate) as required by its Privacy and Security Events Policy and Breach Notification Policy. Audit logs should either be in readable form or translatable by some easy to use tool to be in readable form, and they SHALL be examined with some frequency appropriate to HITE-CT in order to detect improper use, at least quarterly.
- The HITE-CT Privacy and Security Officer SHALL review the generated Audit Logs on a regular basis, at least quarterly, based on an audit criteria developed in advance. Anomalies must be documented and appropriate mitigating action taken and documented. HITE-CT requires that this documentation be retained a minimum of six years.

- All HIE systems must be configured to create Audit Logs that track activities involving electronic Protected Health Information (PHI). The review of information systems shall include software applications, network servers, firewalls and other network hardware and software. All anomalies must be documented and appropriate mitigating action taken and documented. All system logs must be reviewed. The review shall include, but is not limited to, the following types of information: data modification, creation, and deletion.

- External Audits of the HITE-CT infrastructure services shall be conducted at least annually as a minimum requirement, and the comprehensive audit procedures should be developed, documented and available.
  - External systems auditor shall have no conflict of interest
  - External systems auditor is subject to approval by the HITE-CT Board of Directors

- Privacy and Security Audit logs SHALL be available used to support the Privacy and Security Offer in response to inquiry by patients or providers regarding access and disclosures of HITE-CT managed PHI. All HITE-CT participants and infrastructure services maintaining primary Audit records related to the HITE-CT system exchanges SHALL respond to inquiries and investigation of auditable events as requested by the HITE-CT Privacy and Security Officer. .
- External Audits of the HITE-T infrastructure services shall be performed at least annually and when any major system or business changes occur. The evaluation shall include:
  - The generation of a compliance audit findings report,
  - Documentation that an identified deficiency has been addressed, will be addressed in order of priority, or represents a risk the organization is willing to accept,
  - The documentation on the evaluation shall be retained for minimum of six years however some states may have longer retention requirements.

- The Audit Record Repository system SHALL support the following queries:
  - List all HITE-CT users who have accessed or modified a given Healthcare Consumer's PHI in the HITE-CT systems over a given period of time
  - List the identification of all Healthcare Consumers whose PHI has been accessed or modified by a given HITE-CT user over a given period of time
  - List all break-glass events where break-glass is supported
  - List events where information is requested from the HITE-CT systems, but no information is published for the Healthcare Consumer by the provider that requested the information
  - List events that request information marked as sensitive
- For purposes of data authentication the use of a valid date/time stamp is required.
  - All HIE Nodes exchanging PHI SHALL implement the IHE Consistent Time (CT) profile to assure that timestamps and Audit Logs are synchronized
- Audit Logs shall be secure and tamper-proof. Access to system Audit Log analyzing tools and Audit Logs shall be safeguarded to prevent misuse or compromise.
- Information integrity is audited by logging that no change has occurred since the system signature was applied and shall include a valid date/time stamp.
  - Where Audit Logs are signed, for the purposes of data validation, the signer credentials must be from a trusted authority, and the credential must be current and without constraints, and the credential must be of the appropriate type for the requested data (for example physician or pharmacist). To ensure data integrity, credentials shall indicate that no change has occurred since the signature was applied and must have a valid date/time stamp.

- Audit Logs shall be generated by the HITE-CT systems, by the Participating Health Care Subscribers' EHR systems, and by other computer software and systems that communicate with the HITE-CT systems to access, store and communicate Protected Health Information about individuals who have documents registered in the HITE-CT systems.
- As per the Policy on Information Security, PHCSs' EHRs or other provider systems providing information to or retrieving information from HITE-CT systems are expected to create secure Audit Logs whenever PHI is accessed, created, updated, or archived via an EHR or other information system. Audit logging shall be implemented at all times and procedures for analyzing Audit Logs shall be provided and used by the organization managing the Audit Record Repository on behalf of the PHCS.
- Audit Logs accessible by Privacy and Security Officers of PHCS shall be restricted to records of access by the PHCS.

PROCEDURE:

- HITE-CT Audit Logs shall be reviewed on a routine basis, at least quarterly, by the HITE-CT's Privacy and Security Officer and by the Privacy and Security Officers of Participating Health Care Subscribers. Any suspicious activity discovered by HITE-CT shall be reported to the Participating Health Care Subscriber and HITE-CT shall generate a Reportable Event report. Any suspicious activity discovered by a Participating Health Care Subscriber shall be reported to HITE-CT; HITE-CT shall generate a Reportable Event report as per the HITE-CT Breach Notification Policy. The HITE-CT Privacy and Security Officer shall specifically review Audit Logs to detect intrusion attempts and patterns of access to the HITE-CT HIE.
- HITE-CT Audit Logs shall be reviewed by HITE-CT and Participating Health Care Subscriber as needed to follow up on inquiries from providers and patients regarding accesses and use of HITE-CT systems.
- The HITE-CT Privacy and Security Officer SHALL maintain all Audit Report documentation.
- All audit trail records SHALL be maintained electronically and SHALL conform to the IHE Audit Record Repository (ARR) interoperability specification.
- All audit and mitigation activities SHALL be reported to the HITE-CT Board of Directors.
- An individual may request an Audit Report of access to/disclosure of his or her PHI in the HITE-CT systems, occurring within a period no longer than six years prior to the date of request, by contacting HITE-CT's Privacy and Security Officer (privacy_officer@hitect.org). HITE-CT shall provide the requested Audit Report within 30 calendar days, and it shall provide the following information pursuant to 45 CFR § 164.528(b):
    1. The date of access/disclosure;
    2. The name of the PHCS and/or user or other person who received the PHI and, if known, the address of such entity or person;
    3. A brief description of the PHI accessed/disclosed; and
    4. A brief statement of the purpose of the access/disclosure.
- All access and transaction logs shall be kept for six years,

Policy Maintenance

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