HEALTH INFORMATION TECHNOLOGY EXCHANGE OF CONNECTICUT

POLICY AND PROCEDURE

Policy Name/Subject: HITE-CT BREACH NOTIFICATION POLICY V1.0	Policy Number: 7	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 define policy surrounding identification, investigation, notification, and mitigation of a breach of any PHI within the HITE-CT system.

DEFINITIONS:

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 person or entity that performs certain functions or activities for, or provides services to, a Covered Entity (as that term is defined in the Health Insurance Portability and Accountability Act of 1996) that involve the use or disclosure of Protected Health Information

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

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 institution or 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

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.
For breach or potential violations of privacy and security rule, improper use and disclosures that may violate the privacy rule or rise to the level of a breach detection outside of audit.

POLICY:

PHCSs are obligated to report all Reportable Events involving the HITE-CT to their organization's privacy and security officer(s) within ten (10) day of their discovery, who will advise HITE-CT of the Reportable Event.

Other individuals who have information about Reportable Events involving the HITE-CT managed health records are encouraged to file reports or complaints with HITE-CT's privacy and security officer

If Breach occurs at the PHCS level, then any required public notification is responsibility of the PHCS. If the Breach occurs at the HITE-CT level, then the responsibility is of HITE-CT Privacy and Security Officer to report the breach to the PHCS, which will in turn make any required public notifications.

In the case of Breach, it is permissible that HITE-CT access and use MPI information to support contact of the healthcare consumers impacted by that breach in compliance with 74 CFR 162.

Where a breach occurs at PHCS that pertains to HITE-CT managed data, then the PHCS SHALL notify HITE-CT so that an investigation may follow.

When a notification is made, the HITE- CT Privacy and Security Officer SHALL investigate. HITE-CT SHALL notify all PHCSs impacted by the breach

.

HITE-CT will establish and publicize one or more methods for filing reports for PHCS and members of the public.

Upon receipt of a Reportable Event Report or Complaint, HITE-CT's Privacy and Security Officer will log the Reportable Event, acknowledge receipt of the Reportable Event report or complaint to the person who filed it, inform the affected PHCS's privacy and security officer(s) of the event if they do not already have knowledge of it, and begin a review of the event to the extent that it involves HITE-CT. If it appears to HITE-CT's Privacy and Security Officer that there is an imminent threat to data security on the HITE-CT systems, HITE-CT's privacy and security officer will take immediate actions to secure data.

Sanctions, including removal of access privileges may be enforced until the source has mitigated the issue locally or possibly permanently as considered on a case-by-case basis.
The Privacy and Security Officer (s) of the affected PHCPs will cooperate with the Reportable Event review. Once the facts are gathered, HITE-CT's Privacy and Security Officer will determine whether a violation of HITE-CT's privacy and security policies, procedures or relevant federal or state law has occurred.

HITE-CT and the affected PHCPs will collaborate to take steps to correct any weaknesses in their systems, policies, or procedures that were identified during the review. The Privacy and Security Officer (s) of the affected PHCPs will work with HITE-CT's privacy and security officer to consider the need to develop a mitigation plan that is mutually acceptable. The mitigation plan should include steps to prevent the Reportable Event from reoccurring, and may include but not be limited to:

additional employee training and education; facility and computer system changes; and policy revisions.

The HITE-CT Privacy and Security Officer SHALL complete a review completed within thirty (30) days of notice to HITE-CT, and SHALL prepare a report of the Reportable Event documenting the facts gathered from the review, event mitigations, and measures to be taken to prevent recurrence of such an event.

Access monitoring

- The HITE-CT Privacy and Security Officer will monitor Participant access to the HIE at least monthly by reviewing the HITE-CT system-generated audit reports.
- The HITE-CT Privacy and Security Officer will contact the Participant to review any suspicious activity. In case of a Reportable Event, the Privacy and Security Officer will generate a report

Breach Notification

In circumstances where it has been determined that a Reportable Event constitutes a Breach, HITE-CT will notify the PHCS(s) whose patient information was subject to the unauthorized acquisition, access, use or disclosure no later than ten (10) business days following the discovery of the Breach. Such notification will include the time and date of the Breach discovery and the identification of each individual whose PHI is involved.

In the case of an individual breach, HITE-CT SHALL work with the PHCS to reach out to the patient to notify the patient that is the data subject of any breach reported to the organization by HITE-CT within sixty (60) days following discovery of the breach.

In the case of a general breach, HITE-CT SHALL notify those impacted via media, and MAY utilized the EMPI to establish more individualized outreach for notification of a general breach.

The notification to the affected individual(s) will contain, to the extent possible, the following:
1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.
2. A description of the types of unsecured PHI that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, or disability code.)
3. The steps individuals should take to protect themselves from potential harm resulting from the Breach.
4. A brief description of what the PHCS and HITE-CT are doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Policy Maintenance

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