Connecting Connecticut Through Health Information Technology

DRAFT
Privacy and Security Policies for Health Information Exchange

Prepared by

eHealthConnecticut Privacy and Security Advisory Committee

March 26, 2010

Contents

Revision History Table

Version Number	Description of Change	Name of Author	Date Published
Identify V#	*Provide details of each update here to help others in the organization follow changes*	*Name of the person who actually made the changes*	*Date the version was finalized*
V2	Edits/comments	Leah Barry	11/24/09
V3	Edits incorporated into section 301, 304, 405.3 & 405.5	Shirley Neal	11/25/09
V4	Edits to Background and section 301 (mapped Privacy Policy Summary to Section 301 per Scott Cleary's request)	Leah Barry	11/27/09
V5	Edits to entire document	Leah Barry	12/2/09
V6	Edits to reflect changes resulting from 12/3/09 meeting with pilot participants	Leah Barry	12/10/09
V7	Edits to reflect the changes to the patient consent policy	Leah Barry	3/17/10
V8	Prepare draft to post to website	Leah Barry	3/26/10

Background

eHealthConnecticut (eHealthCT) is a collaborative formed in 2006 to create, champion, and sustain a secure, statewide health information exchange (HIE) that will dramatically improve the safety, efficiency, and quality of health care in Connecticut. eHealthCT is a not-for-profit entity representing a collaborative approach to meeting the challenge of health information technology adoption and interoperability for the entire state of Connecticut.

eHealthCT is committed to improving healthcare IT interoperability throughout the state through the implementation of a statewide HIE. To that end, this policy framework defines the policies for community clinical data exchange via the eHealthCT HIE. The policies establish baseline operating rules for the HIE, as the provider of HIE services, and for HIE Participants, as users of the HIE.

Purpose

The following policies provide basic, minimum policy requirements to foster cross organization data exchange via the eHealthCT HIE during the pilot phase of the HIE. These policies establish baseline privacy and security protections for organizations engaged in exchanging electronic health information.

Additionally, these policies function as a set of principles and long-term goals that form the basis of making rules and policy, and gives overall direction, planning, and development to the organization. It serves as the foundation for development of additional policies, procedures, and implementation guides to define additional, more specific requirements for exchanging clinical data as the HIE matures and expands its Participant base.

Definitions

Administrative safeguards: Administrative actions, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic individually identifiable health information and to manage the conduct of the entity's workforce in relation to the protection of that information. Administrative safeguards include policies and procedures, workforce training, risk management plans, and contingency plans.

ARRA/HITECH refers to that portion of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5), specifically Subtitle D, that outlines the obligations of HIEs, including with respect to HIPAA.

Collect/Collection: The acquisition or receipt of information, including individually identifiable health information.

Consent means an Individual's act of giving written permission to a Participant in the eHealthConnecticut Health Information Exchange ("HIE") for the use or disclosure of his or her protected health information in a form which meets all of the requirements set forth in the HIPAA Privacy Regulations,45 CFR $ 164.508.

Corrective measures: Actions taken to address a security breach or privacy violation, with the intent to counteract the breach or violation and reduce future risks.

Covered Entity: The Administrative Simplification standards adopted by Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) apply to any entity that is:

- a health care provider that conducts certain transactions in electronic form (called here a "covered health care provider").
- a health care clearinghouse.
- a health plan.

De-identified means that all identifying information related to an individual as set forth in the HIPAA Privacy and Security Rule,45 CFR Section 164.514 (b), are removed from the protected health information.

Disclose/Disclosure: The release, transfer, exchange, provision of access to, or divulging in any other manner of information outside the person or entity holding the information.

Health Care Operations shall mean activities of a Participant providing treatment to an individual relating to quality assessment and improvement, evaluations relating to the competence of treating providers or necessary administrative and management activities all as defined in the HIPAA Privacy Regulations,45 CFR $164.501.

Health Information: Any information that 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.

HIE is the health information exchange operated by eHealthCT.

Individual represents the person who is the subject of the PHI, but also includes a person who qualifies as a personal representative of the patient in accordance with legal requirements.

Individually Identifiable Health Information: Health information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Open: Actively communicating information through notice or otherwise.

Participant means any health care provider, including any health care organization, that has executed an effective BAA/SLA with the HIE and is registered and authorized to access the eHealthCT HIE.

Persons and Entities: Health care professionals, partnerships, proprietorships, corporations and other types of organizations and their agents when acting on their behalf.

PHI and ePHI: ePHI stands for Electronic Protected Health Information. It is any protected health information (PHI) which is created, stored, transmitted, or received electronically. Protected Health Information (PHI) under HIPAA means any information that identifies an individual and relates to at least one of the following:

- The individual's past, present or future physical or mental health.
- The provision of health care to the individual.
- The past, present or future payment for health care.

Physical safeguards: Physical measures, policies and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. Physical safeguards include workstation security and use procedures, facility security plans, data backup and storage, and portable device and media controls.

Privacy: An individual's interest in protecting his or her individually identifiable health information and the corresponding obligation of those persons and entities, that participate in a network for the purposes of electronic exchange of such information, to respect those interests through fair information practices.

Security: The physical, technological, and administrative safeguards used to protect individually identifiable health information.

Technical safeguards: The technology and the policies and procedures for its use that protect electronic individually identifiable health information and control access to it.

Transparent: Making information readily and publicly available.

Treatment means the provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use: Is the employment, application, utilization, examination, analysis, or maintenance of individually identifiable health information.

Policies

100: Compliance with Applicable Law and eHealthCT HIE Policy

Policy: If there is a conflict between eHealthCT HIE Policies and Participant policies, the policy that is most protective of individual privacy shall govern decision making. This deference to more protective policies echoes the HIPAA federal pre-emption requirements which do not preempt more protective state privacy laws xxx 45 CFR 160.203

1. Laws
    a. eHealthCT shall comply with all federal, state, and local laws, including the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as they pertain to healthcare data exchanged via the HIE.
    b. eHealthCT shall maintain internal policies and procedures for compliance with legal requirements.
    c. Each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights.
    d. Each participant shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure compliance.
    e. Each Participant shall be aware of the provisions of certain state laws which are [may be] more stringent than, and not preempted by, the HIPAA Privacy and Security Regulations.

2. eHealthCT HIE Policies
    a. Each Participant shall, at all times, comply with all applicable eHealthCT HIE policies and procedures ("eHealthCT HIE Policies"). These policies may be revised and updated from time to time upon reasonable notice to the Participant. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these eHealthCT HIE Policies.
    b. In the event of a conflict between these eHealthCT HIE Policies, and an organization's own policies and procedures, the Participant shall comply with the policy that is more protective of individual privacy and security.

3. Participant Policies
    a. Each Participant is responsible for ensuring that it develops the required, appropriate, and necessary internal policies for compliance with applicable laws and eHealthCT HIE Policies.
    b. Each Participant is responsible for documenting these policies in writing and should use these policies to facilitate the training of personnel who will handle health information accessed from the HIE.
    c. In the event of a conflict between these eHealthCT HIE Policies and Participant's own policies and procedures, the Participant shall comply with the policy that is more protective of individual privacy and security.

d. Participants shall be aware of the provisions of certain state lawswhich are [may be] more stringent than, and not preempted by, the HIPAA Privacy and Security Regulations.

200: Notice of Privacy Practices

Policy: Each Participant shall develop and maintain a notice of privacy practices (the "Notice") that complies with applicable law and eHealthCT HIE policies.

1. Content – the Notice shall:
    a. Meet the content requirements set forth under the HIPAA Privacy Rule; **45 C.F.R. 164.520(B)
    b. Include a description of the eHealthCT HIE ; and
    c. Inform individuals regarding:
        i. what information the Participant may include in and make available through the HIE;
        ii. who is able to access the information;
        iii. for what purposes such information can be accessed; and
        iv. how the individual can revoke consent to permit his/her PHI from being accessed in the HIE
2. Provision to Individuals
    a. Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals. The policies and procedures shall be consistent with the eHealthCT HIE Policies and comply with applicable laws and regulations. Each Participant shall update its Notice to describe its participation in the HIE and to inform individuals who Opt-In to sharing data how medical information may be used within the HIE.
    b. For Participants that are healthcare providers, the Notice shall be:
        i. available to the public upon request;
        ii. provided to an individual at the date of first service delivery;
        iii. available at the Participants' organization; and
        iv. posted in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice. 45 C.F.R. 164.520©(2), (3)
4. Individual Acknowledgement
    a. Each Participant that is a health care provider shall make a good faith effort to obtain the individual's written acknowledgement of receipt of the Notice or to document their efforts and/or failure to do so.
    b. The acknowledgement of the Notice shall comply with all applicable laws and regulations
    c. Each Participant shall have its own policies and procedures governing obtaining and acknowledgement of the receipt of the Notice. These policies and procedures shall be consistent with this Policy and comply with the applicable laws and regulations.

5. Participant Choice - Participants may choose a more proactive notice distribution process than provided in the eHealthCT HIE Policies and may include more detail in their Notice.

300: Individual Participation and Control of Information Posted to the HIE

Policy: Individuals will need to provide their healthcare provider with authorization to share their protected health information on the HIE at each encounter with each of their healthcare providers. This authorization will apply to all providers participating in the HIE and all PHI permitted by applicable laws and regulations.

301: Patient Authorization

a. Opt-In Policy: An Individual's choice to participate in the HIE shall be exercised through the Participant, as described in the Participant's Notice. The Individual's choice to opt-in to the HIE must be provided in writing through the Paticipant's patient consent process at each encounter.
    i. This consent permits access to PHI created on the date the authorization was signed.
    ii. This consent permits the re-disclosure of PHI to the extent permitted by applicable laws and regulations.
    iii. An Individual who has signed an authorization to permit his/her PHI to be available through the HIE for treatment purposes shall be entitled to revoke such consent by providing the Participant with written notice of revocation through the Participant's patient consent process.
b. Opt-Out Policy: An Individual's choice not to participate in the HIE shall be exercised through the Participant, as described in the Participant's Notice. The Individual's choice to opt-out of participation or revoke prior consent to participate in the HIE must be provided in writing through the Participant's patient consent process.
    i. PHI of Individuals who do not consent to participate in the HIE will not be available through the HIE.
    ii. An Individual who has chosen not to make his or her PHI available through the HIE subsequently may be included only if the individual chooses to participate in the HIE by signing an authorization to permit his/her PHI to be made available through the HIE.
    iii. An Individual who has previously consented to make his or her PHI available through the HIE may revoke such consent by providing the Participant with written notice of revocation through the Participant's patient consent process.
c. Each Participant shall document and maintain documentation of all individuals' decisions whether to have information about them included in the HIE. Each Participant shall update its own practice management

/EMR system with all individuals' authorization status and will electronically send the transaction to the HIE with the individuals' registration information.

302: Participant Choice

Policy: PHI collected, used or disclosed related to Individuals will be supported by the Participants internal policy on the care and access to PHI. These policies will include, but are not limited to:

a. reasonable and appropriate processes to enable the exercise of a Individual's choice not to participate in the HIE data exchange;
b. details about the information created, collected, used and disclosed;
c. the purpose and limitations of the use of the information;
d. the Individual's right to access and correct their PHI;
e. processes related to the access and correction of the Individual's PHI;
f. the right to request and receive in a timely and intelligible manner information regarding who has that individual's PHI and what specific data the party has; to know any reason for a denial of such request; and
g. the Individual's right to challenge or amend any personal information.

303: Provision of Coverage or Care

Policy: Participants shall not withhold coverage or care from an individual on the basis of that individual's choice not to have information about him or her included in the HIE.

304: Patient Education Materials

Policy: eHealthCT has developed patient educational materials to be used by Participants to educate Individuals about the HIE.

Participants may use these educational materials provided by eHealthCT to inform Individuals about the HIE, the benefits of HIE, and the Individual's right to choose whether or not to participate.

400: Uses and Disclosures of Health Information

401: General Use and Disclosure

Policy:

a. All Individual PHI in the HIE will be available for public health and quality reporting. The Privacy Rule permits covered entities to disclose protected health information, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health

surveillance, investigations, or interventions. See 45 CFR 164.512(b)(1)(i).

b. PHI shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. In General, requests for disclosure of and/or use of health information for treatment, payment, and the health care operations of a covered entity, as each is defined by HIPAA will be permitted [45] V>F>R> 164.503(1)(ii)

402: Compliance with Law

Policy:

a. All disclosures of health information through the HIE and the use of information obtained from the HIE shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful discriminatory purpose.

b. If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing health information for a particular purpose, the requesting Participant shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of such at the request of the disclosing Participant [**] See 45 C.F.R.164.530.(j).

403: Purposes

Policy: In general, requests for use of health information for treatment, payment, and the health care operations of a covered entity in the HIE, as each is defined by HIPAA, will be permitted. Furthermore, subject to certain limitations and under certain circumstances including but not limited to, using health information for law enforcement, disaster relief, research, and public health purposes also is permissible. Use of PHI through the HIE for marketing or marketing-related purposes is prohibited without specific Individual authorization.

a. PHI shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

b. A Participant may request health information through the HIE only for purposes permitted by applicable law.

c. Each Participant shall provide or request health information through the HIE only to the extent necessary and only for those purposes that are permitted by applicable federal, state, and local laws and regulations and these eHealthCT HIE policies. [45 C.F.R.164.502(a), (b)]

d. Under no circumstances may information be requested for a discriminatory purpose.

e. In the absence of a permissible purpose, a Participant may not request information through the HIE.

404: eHealthCT HIE Policies

Policy:

a. eHealthCT shall execute a DURSA with each Participant prior to beginning live exchange of data. The DURSA shall establish the mutual responsibilities of eHealthCT and the Participant for compliance with the policies in this document and shall be amended as needed.
    i. eHealthCT shall comply with all provisions of the DURSA.
    ii. eHealthCT shall participate annually in a review with each Participant of the DURSA and related policies, agreements, requirements, and best practices.
    iii. eHealthCT shall administer disciplines for non-compliance with data sharing agreements up to and including termination of a Participant's participation in HIE.
b. PHI shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
c. ARRA directs Covered Entities to provide individuals access to certain information in electronic format.
d. ARRA provides new restrictions on marketing use of PHI. HIPAA Covered Entity or Business Associate may not receive remuneration in exchange for any PHI without authorization from individual.
e. Uses and disclosures of and requests for health information via the HIE shall comply with all eHealthCT HIE Policies, including but not limited to, the eHealthCT Policy on Minimum Necessary and the eHealthCT Policy on Information Subject to Special Protection. **45 C.F.R. 164.502.(b)
f. Information Use: Use of electronic health records for clinical research (electronic case report forms) and related secondary use cases such as safety reporting, disease registries, bio-surveillance, lab, and image exchange, and post-marketing surveillance shall comply with state and federal law.
g. Information disclosure: The HIE is only to serve as intermediary among HIE Participants for exchange of clinical data, and as such, the HIE is not authorized to release PHI for any reason unless authorized to do so by written agreement with a Participant.
h. In the event that de-identified PHI is requested for clinical research from data maintained for the HIE, eHealthCT, through its Executive Committee or its designee Committee, shall review and approve or disapprove the request. (See Disclosure of Individual Information for Secondary Use section 407.2 and Research Section 410)

405: Participant Policies

Policy: Each Participant is responsible for ensuring that it develops the required, appropriate, and necessary internal policies for compliance with applicable laws and these eHealthCT HIE Policies.

a. Participants shall execute a DURSA with eHealthCT prior to beginning live exchange of data. The DURSA shall establish the mutual responsibilities of eHealthCT and the Participant for compliance with the policies in this document and shall be amended as needed.
    i. Participants shall comply with all provisions of the DURSA
    ii. Participants shall participate annually in a review with eHealthCT of the DURSA and related policies, agreements, requirements, and best practices.
    iii. Participant shall make best efforts to comply with best practices agreed upon by eHealthCT and Participants.
    iv. Participants shall execute annually a "Statement of Compliance with the DURSA, policies, agreements, requirements, and best practices.
b. Each Participant shall refer to and comply with its own internal policies and procedures regarding disclosures of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making such disclosures
c. Each Participant is responsible for using written documentation of their internal policies and the eHealthCT HIE Policies to facilitate the training of personnel who will handle PHI and
d. All Participants shall have policies and procedures to ensure that only those involved in the diagnosis or treatment of an individual, payment for that treatment or necessary health care operations may access the individual's PHI on the HIE. Participants shall comply with the HITECH Act of 2009 and HIPAA privacy and security rule and all applicable state laws.
e. eHealthCT may provide guidance to Participants detailing the permissibility or impermissibility of requesting or using health information for certain specified purposes under applicable law.
f. The HIE shall provide notification to Participants who access PHI on the HIE substantially similar to the following statements:

- In the event that information released from the HIE is protected by the HHS Confidentiality of Alcohol and Drug Abuse Patient Records Regulations: This information has been disclosed to you from records protected by Federal confidentiality rules, 42 CFR Part2, which prohibit you from making further disclosure unless further disclosure is expressly permitted by the written consent of the person to whom it pertainsl or as otherwise permitted by the 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict use of information protected under 42 CFR Part2 from criminalnvestigations or prosecutions of an alcohol or drug abuse patient.

- In the event that information released from the HIE constitutes psychiatric information protected under Connecticut Law: This information has been disclosed to you from records whose confidentiality is protected by state law. State law prohibits you from making any further disclosure of it or of using it for any purpose other than [need to define] without the specific written consent by the person to whom it pertains, or as otherwise permitted by said law.

- In the event that information released from the HIE constitutes confidential HIE related information protected under Connecticut Law: This information has been disclosed to you from records whose confidentiality is protected by state law. State law prohibits you from making any further disclosure of it without the specific written consent of the person to whom it pertains, or as otherwise permitted by said law. A general authorization for the release of medical or other information is NOT sufficient for this purpose.

406: Privacy Provisions to Business Associates

Policy: eHealthCT shall execute a BAA with each Participant prior to beginning live exchange of data. The BAA shall establish the mutual responsibilities of eHealthCT and the Participant for compliance with the policies in this document and shall be amended as needed. The BAA shall include new provisions required by the HITECH Act including but not limited to:

a. additional provisions of the Privacy Rule
b. HIPAA civil and criminal penalties for business associates that violate privacy provisions
c. Business Associates are now subject to the same HIPAA privacy and security provisions and penalties that apply to Covered Entities (CEs).

407: Information Disclosure

Policy:

a. Disclosure of Individual Information Not Requiring Written Authorization
    i. The HIE shall not release or disclose any PHI except as required by law or as defined in the DURSA
    ii. HIE Participants shall maintain and follow internal policies which shall govern release and disclosure of PHI.
b. Disclosure of individual Information for Secondary Use
    An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Privacy Rule. However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.
    i. Reasonable Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as those that limit incidental uses or disclosures. See 45 CFR 164.530(c).
    ii. eHealthCT shall not release or disclose PHI except as required by law or as defined in the DURSA
    iii. Participants shall maintain and follow internal policies which shall govern release and disclosure of PHI

c. Disclosure of Sensitive Health Information
    i. Responsibility for restricting the Transmission of Sensitive health Information will reside with the Sending Participant.
    ii. The Sending Participant shall obtain appropriate Individual consent, if required, prior to transmitting Sensitive Health Information and shall transmit such information and only if such consent has been obtained.

408: Accounting of Disclosures

Policy: Individuals have the right to request an accounting of disclosures of their health information made through an electronic record. eHealthCT, upon request, must provide Individuals with a record of the entities to whom they have disclosed the Individual's PHI.

a. Participants will be responsible for responding to Individual requests for reporting of disclosures of their PHI. eHealthCT will support this requirement by making available the content of logs maintained by the HIE for use in the Participants' disclosure reporting process.
b. eHealthCT shall make available to Participants who are parties to a clinical data transmission all log data maintained by the HIE that pertains to the transmission.
c. eHealthCT shall establish a process and specifications for accessing of log information by authorized Participant staff.
d. Participants shall maintain internal policies for reporting to individuals regarding PHI disclosures.
e. Participants shall be responsible for responding to Individual requests for disclosure and may use data in the HIE to respond to such requests.
f. Participants shall have the ability to report to Individuals all disclosures represented in internal and HIE logs for not less than three years from the date of access to Individual data.

409: Breach of Disclosure Policy

Policy: In the event that the HIE becomes aware of any actual or suspected breach, either through notification by a Participant or otherwise, eHealthCT shall:

a. Notify any Participants whose data is affected by the breach
b. Investigate (or require the applicable Participant to investigate) expediently and without unreasonable delay the scope and magnitude of such actual or suspected breach, and identify the root cause of the breach.
c. Mitigate (or require the applicable Participant to mitigate) to the extent practicable, any harmful effect of such breach that is known to eHealthCT or the Participant. eHealthCT's mitigation efforts shall correspond with and be dependent upon its internal risk analyses.
d. Notify (or require the applicable Participant to notify) the Individual and any applicable regulatory agencies as required by federal, state and local

laws and regulations, except if a law enforcement agency determines that such notification impedes a criminal investigation.

e. Participant shall maintain and uphold individual policies for the notice of misuse or breach of policies.
f. Participant shall appropriately train its personnel and inform them of sanctions and other action that will result from any breach of confidentiality.
g. Participant shall report any breaches and/or security incidents to the particular Participant or External Trading Partner whose data was improperly used. Notification shall be made in writing and in the most expedient time possible and without unreasonable delay.
h. Participant shall report to eHealthCT any actual or suspected breach of confidentiality. Notification shall be made in writing in the most expedient time possible and without unreasonable delay.
i. Participant shall notify the Individual whose health information was disclosed in breach of policy.

410: Research

Policy:

a. eHealthCT or its Participants are permitted to disclose individual health information to public agencies, clinical investigators, including clinical investigators conducting epidemiological studies, health care research organizations, and accredited public or private nonprofit educational or health care organizations for bona fide research purposes provided that: *[Reference: 45 C.F.R. § 164.512(i)(1) & relevant CT Code]*
b. In the event that de-identified PHI is requested for clinical research from data maintained for the the HIE, eHealthCT , through its Executive Committee, or its designee Committee shall review the request to determine if it should be approved.
c. In making its determination, the Committee may consider any Institutional Review Board approval supporting the request. If approved, eHealthCT , through an approved Data Subcontractor, shall prepare the de-identified PHI requested and shall be reimbursed for its expenses by the requesting party.
d. The requesting party shall be required to provide contract assurances that no attempt shall be made by it to “identify” the de-identified PHI from eHealthCT provided for the approved research.
e. eHealthCT shall make available upon request an annual report of all approved requests for de-identified PHI from the HIE, including the date of the de-identified data release, the entity to which the data was released and a summary of the research involved.

500: Information Subject to Special Protection

Policy: Participants' collection, use, and disclosure of health information will be limited to legitimate purposes and will defer to the law or policy most protective of an individual's privacy.

1. Some PHI may be subject to special protection under federal, state, and/or local laws and regulations (e.g., substance abuse, behavioral health, and HIV).
2. Each Participant shall determine and identify what information is subject to special protection under applicable law prior to disclosing any information through the HIE.
3. Categories that may warrant a higher degree of security in an EHR system
    a. Individual type and identity
    b. Diagnosis or condition
    c. Procedures or testing
    d. Consent and custody
    e. Research
4. Each Participant is responsible for complying with such laws and regulations.

600: Minimum Necessary

Policy: eHealthCT will implement reasonable minimum necessary policies and procedures to limit how much protected health information is used, disclosed, and requested for certain purposes. These minimum necessary policies and procedures limit who within the entity has access to PHI and under what conditions based on job responsibilities and the nature of the business.

1. Uses
    a. Data use must be limited to the amount necessary to accomplish specified purposes. Minimization of use will help reduce privacy violations, which can easily occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes
    b. Each Participant shall share PHI obtained through the HIE and allow access to such information by only those workforce members, agents, and contractors who need the information in connection with their job function or duties.
2. Disclosures
    a. Each Participant shall disclose through the HIE only the minimum amount of PHI as is necessary for the purpose of the disclosure.
    b. Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy
3. Requests
    a. Each Participant shall request only the minimum amount of PHI through the HIE as is necessary for the intended purpose of the request.
    b. This Minimum Necessary Policy does not apply to requests by health care providers for treatment purposes.
4. Entire Medical Record
    a. A Participant shall not use, disclose, or request an individual's entire medical record except where specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

b. This limit does not apply to disclosures to or requests by a health care provider for treatment purposes or disclosures required by law.

700: Workforce, Agents, and Contractors

Policy:

1. Access to System - No workforce member, agent or contractor shall be provided with access to the HIE without first having been trained on Participant Policies and eHealthCT HIE Policies.
2. Training
    a. Each Participant shall develop and implement a training program for its workforce members, agents, and contractors who will have access to the HIE to ensure compliance with eHealthCT HIE policies. **45 C.F.R. 164.530(b)
    b. The training shall include a detailed review of applicable Policies to include, but not limited to:
        i. confidentiality of PHI under the HIPAA Privacy and Security Regulation and all other applicable federal and state laws and that they are obligated to protect PHI in compliance with such laws and eHealthCT HIE Policies;
        ii. only access the HIE for purposes of treatment of an individual or necessary health care operations;
        iii. hold any passwords, or other means for accessing the HIE, in a confidential manner and to release them to no other individual;
        iv. comply with both eHealthCT HIE Policies and those of the Participant, and that they understand that their failure to do so may result in their exclusion from the HIE and may constitute cause for disciplinary action.
    c. Each workforce member, agent, and contractor shall sign a representation that he or she received, read, and understands these eHealthCT HIE Policies.
3. Discipline for Non-Compliance
    a. Each Participant shall implement procedures to discipline and hold workforce members, agents, and contractors accountable for ensuring that they do not use, disclose, or request health information except as permitted by these Policies and that they comply with these Policies. **45 C.F.R. 164.530(e)
4. Reporting of Non-Compliance
    a. Each Participant shall have a mechanism for, and shall encourage, all workforce members, agents, and contractors to report any non-compliance with eHealthCT HIE Policies to the Participant. **45 C.F.R. 164.530(e)
    b. Each Participant also shall establish a process for individuals whose health information is included in the HIE to report any non-compliance with eHealthCT HIE Policies or concerns about improper disclosures of information about them.

800: Amendment of Data

Policy: Each Participant shall comply with applicable federal, state, and local laws and regulations regarding individual rights to request amendment of PHI. **45 C.F.R. 164.526

1. A Participant shall permit an individual to request that the Participant make an amendment to his/her health information maintained by the entity. The entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements. [*Reference: 45 .F.R.§164.526(b)(1)]*
2. A Participant shall act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows. . [*Reference: 45 C.F.R.§164.526(b(2))*
    a. If the entity is unable to act on the amendment within the time required, the entity may extend the time for such action by no more than 30 days, provided that:
    b. The entity provides the individual with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request; and
    c. The entity may have only one such extension of time for action on a request for an amendment
3. An entity may deny an individual's request for amendment, if it determines that the individual PHI or record that is the subject of the request: [*Reference: 45 C.F.R.§164.526(a)(2)]*
    a. Was not created by the entity, unless the individual provides a reasonable basis to believe that the originator of the individual health information is no longer available to act on the requested amendment;
    b. Is not part of the entity's records;
    c. Would not be available for inspection by the Secretary of Health and Human Service, or
    d. Is accurate and complete.
4. An entity may not deny an individual's request to have an addendum added to his/her designated record set.
5. If an individual requests, and the Participant accepts, an amendment to the PHI about the individual, the Participant shall make reasonable efforts to inform other Participants that accessed or received such information through the HIE.
6. The Participant shall notify the recipient Participant within a reasonable time, if the recipient Participant may have relied or could foreseeable rely on the information to the detriment of the individual.

900: Mitigation

Policy:

1. Each Participant shall implement a process to mitigate, and shall mitigate and take appropriate remedial action to the extent practicable, any harmful effect that is known about the use or disclosure of health information that is in violation of: 91)

Applicable laws and/or regulations; (2) Participant policies; (3) eHealthCT HIE Policies, its workforce members, agents, and/or contractors,

2. An entity shall mitigate, to the extent practicable, any harmful effect that is known to the entity of a use or disclosure of individual health information in violation of its policies and procedures or the requirements of the policies and procedures by the entity or its business associate. [*Reference: 45 C.F.R. § 164.530(f)]*
3. An entity shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity; and document security incidents and their outcomes.*[Reference: 45 C.F.R.§ 164.308(a)(6)]*
4. An entity shall have the capability to identify substantiated fraudulent activity within their records and be able to view and/or provide records internally and externally as though the fraudulent activity had not occurred

1000: Technical Security Safeguards and Controls

Policy:

1001: General

Policy:

a. Individually identifiable health information shall be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
b. The HIE shall maintain a secure environment for all its systems that handle Individual data and any centralized data repositories containing Individual or Participant data, including implementing and enforcing appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all data.
c. Participants shall maintain a secure environment for eHealthCT HIE-related infrastructure, services, and data to support the secure and reliable operation and continued development of the HIE, including implementing and enforcing appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all data accessed through the HIE services.
d. Participant shall employ security controls that meet applicable industry or federal standards so that the information and data being transmitted shall not introduce any viruses, worms, unauthorized cookies, Trojans, malicious software, or ‘malware’. In the absence of applicable industry standards, each Participant shall use all commercially reasonable efforts to comply with the requirements of this policy.
e. Participant shall collaborate with eHealthCT to develop security policies and to amend, repeal, or replace provisions as necessary to support the secure operation and continued development of the network.
f. Participant shall conduct periodic reviews, not less that once in a calendar year, of Participant’s internal security, for example, logs, access reports, and incident tracking, and make results of the review available to eHealthCT.

1002: User identification and Authentication

Policy: To prevent unauthorized access of information and maintain data integrity and quality, the authentication provision requires that both the identity and the authority of an entity requesting health information be verified and authenticated, integrating requirements from the HIPAA Privacy and Security Rule. ** 45 C.F.R. 164.514(H), 164.312(D)

a. Each Participant shall follow uniform minimum authentication requirements for verifying and authenticating those within their Participants who shall have access to, as well as other Participants who request access to, information through the HIE.
b. The HIE information system uniquely identifies and authenticates users (or processes action on behalf of users).
c. The HIE information system employs multifactor authentication for remote system access that is NIST Special Publication 800:63 [Section: organization-defined level 3, level 3 using a hardware authentication device, or level 4] compliant.
d. The HIE information system employs multifactor authentication for local system access that is NIST Special Publication 800:63 [Section: organization-defined level 3, or level 4] compliant.
e. The HIE employs multifactor authentication for remote system access that is National Institute of Standards and Technology (NIST) Special Publication 800:63 level 4 compliant.
f. The HIE information system identifies and authenticates specific devices before establishing a connection.
g. Participants shall authenticate all system Users before the User is given access to any HIE resource containing Individual data. Such authentication shall be implemented using an authentication methodology that meets the minimum technical requirements for Authentication Assurance level 2 set forth in NIST Special Publication 800-63
h. The HIE information system obscures feedback of the authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
i. Participant shall assign each System User with access to HIE services to a specific Role as defined by the HIE
j. Participant shall communicate and authenticate credentials. In any data exchange, the Participant shall communicate its credentials, and the HIE shall use such credentials to authenticate the Participant is an HIE Participant in good standing.
k. The HIE Information System shall verify that the user accessing the received Individual Information has a Role that is permitted to access the type of data being requested from the Sending Participant
l. Participant shall include in each request for Individual data a non-repudiable assertion as to the identity and role of the system User who will receive the data.

m. Participant shall maintain policies and procedures that govern Users' ability to access information on or through the Participant's system and through the HIE services.
n. A Participant shall have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the Participant or eHealthCT. Participants shall document the sanctions that are applied, if any. [*Reference: 45 C.F.R.§164.530(e)]*
o. A Participant shall impose appropriate sanctions for work force members who violate security policies or make improper use of Individual Information, including revocation of a User's authorization to access the network as may be appropriate under the circumstances.
p. Participant shall provide its Participant Access Policies to any other Participant upon reasonable request.

1003: Access Control

Policy: The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [organization-defined frequency].

a. Participants must complete appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access. Participants shall review and update the agreements, no less than annually.
b. The Participant shall develop, disseminate, and periodically review/update the following:
    i. a formal, documented, access control policy that addresses, purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and
    ii. a formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
c. Access control policies are tied to specific user roles that link specific user roles to the types of documents that these users are permitted access.
    i. eHealthCT shall establish "Roles" for all Users, which define categories of Users of HIE services. These categories are based on the types of Individual data that these users need to access to perform their job functions, and the permitted purposes for such access.
    ii. Access Privileges are governed by the Role of the User in the Participant organization to which the clinical message is addressed. For example: A User may be the Primary Care Physician of a Individual in one clinic, authorized to view the full longitudinal health record in a message addressed to that clinic. The same User may play a specialist Role in another Participant organization where messages are filtered to display only data needed for permitted purpose.

iii. The permitted purposes are based on each User's job function and relationship with the Individual. HIE Roles are used as community standard classifications to enable sending and Receiving Participants to establish access control rules that are meaningful to each other. The HIE will initially favor simple, broad Role definitions to facilitate adoption by Participants and will refine these definitions over time.

d. Account Management
    i. Establishing, activating, modifying, reviewing, disabling, and removing accounts - review information system accounts, at a minimum, on an annual basis
        (1) The organization employs automated mechanisms to support the management of information system accounts
        (2) The information system automatically terminates temporary and emergency accounts after [organization-defined time period for each type of account].
        (3) The information system automatically disables inactive accounts after [HIO-defined time period]
        (4) The organization employs automated mechanism to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.
    ii. Access Enforcement
        (1) The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy
        (2) The information system restricts access to privileged functions(deployed in hardware, software, and firmware and security-relevant information to explicitly authorized personnel.
    iii. Remote Access – The organization:
        (1) authorizes, monitors, and controls all methods of remote access to the information system;
        (2) employs automated mechanisms to facilitate monitoring and control of remote access methods;
        (3) uses cryptography to protect the confidentiality and integrity of remote access sessions;
        (4) controls all remote accesses through a limited number of managed access control points; and
        (5) permits remote access for privileged functions only for completing the operational needs and documents that rationale for such access in the security plan for the information system.

e. Portable and mobile devices – The organization:
    i. establish usage restrictions and implementation guidance for organization-controlled portable and mobile devices, and
    ii. authorizes, monitors, and controls device access to organization information systems.

f. Unsuccessful login attempts

i. The information system enforces a limit of [organization-defined number] consecutive invalid access attempts by a user during a [organization-defined time period] time period.
ii. The information system automatically:
(1) locks the account/node for an [organization-defined time period, or
(2) delays next login prompt according to [organization-defined delay algorithm] when the maximum number of unsuccessful attempts is exceeded.

g. System use notification
i. message provides appropriate privacy and security notices
ii. based on associated privacy and security policies or summaries
iii. remains on the screen until the user takes explicit actions to log on to the information system.

h. Session Lock
i. The information system prevents further access to the system by initiating a session lock after [organization-defined time period] of inactivity
ii. The session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

i. Session termination – The information automatically terminates a session after [organization-defined time period] of inactivity.

j. Supervision and review – The organization:
i. supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls; and
ii. employs automated mechanisms to facilitate the review of user activities.

k. Permitted activities without identification or authentication – The organization:
i. identifies and documents specific user actions that can be performed on the information system without identification or authentication, and
ii. permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

l. Use of external information systems
i. Establish terms and conditions for authorized individuals to:
ii. access the information system, from external information system
iii. process, store, and/or transmit organization-controlled information using an external information system.
(1) Prohibits authorized individual from using an external information system to access the information system or to process, store, or transmit organization controlled information except in situations where the organization
(2) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan, or
(3) has approved information system connection or processing agreements with the organization entity hosting the external information system.

1004: Audit and Accountability – Auditing access to Individual Information

Policy:

a. eHealthCT shall establish a formal, documented, audit and accountability policy that addresses purposes, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and
b. formal, documented procedures to facilitate the implementation of the audit and accountability policy, and associated audit and accountability controls.
c. eHealthCT shall publish Implementation Guides that shall specify requirements for logging of messages pertaining to Individual data transmitted via the HIE. Implementation Guides shall contain general requirements for logging all messages to include, but not limited to:
    i. Log-In Monitoring:
        (1) 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 HIE. This includes all attempted and failed logons.
        (2) The generated audit logs must be reviewed on a regular basis that is based on an audit criteria developed in advance. Anomalies must be documented and appropriate mitigating actions and documents.
        (3) eHealthCT will retain this documentation for a period of time that is in compliance with its risk management policies and Connecticut state laws as defined by the .
    ii. Information Systems Logs:
        (1) All HIE systems must be configured to create audit logs that track activities involving electronic PHI.
        (2) The review of information systems shall include software application, network servers, firewalls, and other network hardware and software.
        (3) The generated audit logs shall be reviewed on a regular basis based on audit criteria developed in advance. All anomalies must be documented and appropriate mitigating action taken and documented. All system logs must be reviewed.
        (4) The review shall include, but not be limited to, the following types of information: data modification, creation, and deletion.
        (5) eHealthCT will retain this documentation for a period of time that is in compliance with its risk management policies and Connecticut state laws. (Organization-defined period of time)
        (6) Information system reviews should be conducted on a regular and periodic basis, as defined by eHealthCT.
        (7) The HIE system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events, and

(8) provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.
(9) The HIE information system provides time stamps for use in audit record generation. The organization synchronizes internal information system clocks [organization-defined frequency].

iii. Log records shall contain, at a minimum, the following information:
(1) The identity of the Individual whose information was accessed
1. A subset of the demographic information used to find a person should be logged to identify the subject of care
(2) The identity of the user accessing the Individual data
(3) The identity of the Participant with which the User is affiliated, and through whose system HIE services were accessed
(4) The type of Individual data or record accessed (e.g., pharmacy data, laboratory data, etc.) with 'sensitive data specifically identified.
(5) The date and time of access
(6) The source of the Individual data (i.e., the Participant from whose system the accessed Individual data was derived)
(7) eHealthCT shall maintain logs of all messages that pass through its systems for a period of time that is in compliance with the business needs of eHealthCT and is in compliance with state and/or federal law – (Organization-defined period of time)

iv. eHealthCT shall consider logs to be PHI and secure them accordingly.
v. Log records shall support reporting to Individuals and other stakeholders of all disclosures of Individual data via the HIE. Future enhancements may include alerts, alarms, and analysis

d. Security Audit Practice:
i. Audits shall be conducted at least annually as a minimum requirement.
ii. Audits shall provide the capability to compile audit records from multiple components throughout the system into a system-wide [logical or physical], time-correlated audit trail; and
iii. provides the capability to manage the selection of events to be audited by individual components of the system.
iv. Protection of audit information – the information system protects audit information and audit tools from unauthorized access, modification, and deletion.
v. Audit storage capacity – the organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded

e. Audit monitoring, analysis, and reporting – the organization employs automated mechanisms to:

i. integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities, and
ii. alert security personnel of the following inappropriate or unusual activities with security implications:[organization-defined list of inappropriate or unusual activities that are to result in alerts].
(1) The evaluation shall include:
1. The generation of a compliance audit findings report
2. Documentation that an identified deficiency has been addressed, will be addressed in order of priority, or represents a risk eHealthCT is willing to accept.

f. Audit retention – the documentation on the evaluation shall be retained for a minimum of six years to:[45 C.F.R.164.316]
i. provide support for after-the-fact investigations of security, and
ii. meet regulatory and organization information retention requirements.

g. Information Access
i. Audit Controls: Under HIPAA security standards, technical safeguards are required including policy, data, and system requirements. eHealthCT and its Participants must implement technical processes that accurately record activity related to access, creation, modification and deletion of electronic PHI

1005: Data Assurance

Policy:

a. eHealthCT and its Participants shall take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
b. eHealthCT and its Participants shall protect individual health information from unauthorized alteration or destruction.
c. eHealthCT and its Participants shall implement technical security measures to protect against unauthorized access to individual health information that is being transmitted over an electronic communications network. [*Reference: 45 C.F.R.§164.312(c)(1)] & : 45 C.F.R.§164.312(e)(1)]*
d. eHealthCT and its Participants shall implement a mechanism to provide the ability to encrypt and decrypt where appropriate, to protect individual health information . [*Reference: 45 C.F.R.§164.312(a)(2)(iv)]*
e. eHealthCT shall avoid the use of proprietary encryption algorithms, unless reviewed by qualified experts outside of the vendor in question and approved by Federal guidelines. Asymmetric crypto-system keys shall be of a length that yields equivalent strength. eHealthCT's key length requirement will be reviewed annually and upgraded as technology allows.
f. eHealthCT shall implement security measures to safeguard electronically transmitted individual health information being improperly modified without detection until disposed. This includes implementation of electronic mechanisms to corroborate that

individual health information has not been altered or destroyed in an unauthorized manner. [*Reference: 45 C.F.R.§164.312(e)(2)(v)] & 45 C.F.R.§164.312(c)(2)]*

g. eHealthCT shall develop processes to detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable health information.

Attributions

Clear attribution is given to the following sources:

1. Connecting for Health. "The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange." Available online at www.connectingforhealth.org/commonframework
2. NHIN Connect NHIE Gateway Integrated Information Technology Plan – 12/04/08; Federal Health Architecture
3. HISPC collaboration. Appendix A: Uniform Security Policy. March 31, 2009
4. Nationwide Privacy and Security Framework For electronic Exchange of Individually Identifiable Health Information. December 15, 2008. Office of the National Coordinator for HIT. U.S. Department of Health and Human services
5. California Office of Heath Information Integrity (CalOHII)

   Following is CalOHII's analysis of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) portion of the American Recovery and Reinvestment Act of 2009.

   HITECH Act Summary (PDF-26K)

   HITECH Act Summary Matrix (PDF-161K)
   Note: This is a new version and we will be updating the document as new information is released.

   Final HITECH Portion of ARRA (DOC-346K)

6. American Health Information Management Association (AHIMA)
   a. AARA & Electronic Records & HIPAA & Privacy and Security | Blog Entry: posted by Kevin Heubusch March 25, 2009 10:19 am:
   b. Journal of AHIMA Practice Brief Attachment 5/2/2009 Sample Sanctions Determination Document
   c. Journal of AHIMA, Mar 25, 2009 10:19 am | posted by Kevin Heubusch | ARRA & Electronic records & HIPAA & Privacy and security
7. Federal Computer Week - Law requires health data breach notifications - By Ben Bain Feb 27, 2009
8. "http://en.wikipedia.org/wiki/Security_breach_notification_laws"