ClinicalConnect

Principles for Establishing a Practical Cyber Security Incident Management Process in your HIE

John Houston
Vice President, Privacy and Information Security; Assistance Counsel
UPMC

Background - HIPAA

- Most HIEs have established themselves as HIPAA Business Associates of the participants that they serve.
- As a Business Associate, the HIE already has an significant HIPAA compliance obligations, including implementing appropriate security controls as described in HIPAA.
- Compliance with these security controls necessitate that the HIE have an effective incident management process in place.

Background - HIPAA

- **§164.504(e)(2)(ii)(C)** Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware including breaches of unsecured protected health information as required by §164.410.
- **§164.530(f)** A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

General Concepts

- Use HIPAA, “meaningful use” criteria and other regulations as the benchmark – ***nothing more***.
- Being overly proscriptive is the deadly.
- The Federal Data Use and Reciprocal Support Agreement (DURSA), or similar agreement, can provide additional guidance.
- Uniform “obligations” of participants is necessary.
- Operational flexibility is critical.
- Patient transparency is critical.

Benchmarks

- HIPAA, “meaningful use” criteria and other regulations provide a good benchmark for what participants are already obligated to comply with.
- While HIEs often want more rigorous standards, deviation from what participants are already required to do can cause problems due to inconsistency.
- Consistency with benchmarks will result in more consistent compliance.

DURSAs

- The Federal Data Use and Reciprocal Support Agreement (DURSA), or similar agreement, can provide additional guidance regarding what the Federal Government expect when exchange occurs at the national level.
- These standards are more proscriptive than HIPAA.

Uniformity

Uniformity is necessary to ensure that the HIE is able to operate in an efficient and practical fashion.

- Standard agreements executed by all participants.
- Uniform notices.
- Consistent policies and standards of conduct.

Operational Flexibility

While uniformity is vital, their must be sufficient flexibility to support:

- Variations between Participants' operations.
- Variations between how different HIEs are structured and operate.
- Technology differences and "evolution".
- Changes in standards & laws.
- Changes in threats.

Avoid Being Overly Proscriptive

- There is often a desire to demand compliance with extremely detailed and draconian security requirements.
- Providers will differ in size and complexity, making compliance with very specific / detailed requirements difficult.

Patient Transparency

Patient must have an opportunity to understand:

- how their information will be used and managed.
- What safeguards the HIE has established to protect their data.
- How the HIE will address breaches that may occur.

CCHIE Background

CCHIE Security Infrastructure and Knowledge

- ClinicalConnect HIE “leverages” UPMC security and privacy infrastructure & knowledge.
- Servers are hosted within UPMC data centers and thereby inherit the UPMC security infrastructure.
- Access to UPMC Information Security expertise.

Patient Participation

- Opt-out model (i.e. the data is exchanged unless the patient requests to not participate).
- Opt-out model is consistent with Pennsylvania state law.
- Patient's participation decision (consent) is captured through each Participant's registration system.
- The ClinicalConnect master person index tracks all consent decisions and honors the last consent received.

Data Exchange Agreement

- Establishes standards for the exchange of information though the HIE.
- Describes the HIE's and each Participant's rights and obligations.
- Permits exchange for treatment, payment, healthcare operations, public health and the reporting of clinical quality measures (including measures to demonstrate "meaningful use").
- Requires board approval for various other uses, such as benchmarking & comparative purposes, population management and preventative care by the HIE or Provider.

Data Exchange Agreement

- The Data Exchange Agreement must be agreed to without modification by each Participant.
- Can be used as a “Standalone” agreement for Participants that are not members.
- Developed based on input from the HIE’s Privacy Workgroup.
- Approved by the ClinicalConnect Board of Directors.
- Reviewed by outside counsel.
- Requires the use of standard language in each Participant’s treatment consent form.

Data Exchange Agreement

- CCHIE is accountable for investigating breaches.
- Participants are required to report suspected. breaches that they become aware of, as well as to assist as appropriate in the investigation of suspected breaches.

Data Exchange Agreement

Breach Notification.

Provider agrees that on an expedited basis, and in no case longer than within three (3) days of discovering information that leads Provider to reasonably believe that a Breach may have occurred, it will alert the HIE and other HIE Participants whose Health Data may have been Breached. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a Breach occurred, Provider will notify all HIE Participants likely impacted by the Breach and the HIE of such Breach. The notification should include sufficient information for the HIE Participants and the HIE to understand the nature of the Breach. For instance, such notification could include, to the extent available at the time of the notification, the following information:

- One or two sentence description of the Breach
- Description of the roles of the people involved in the Breach (e.g. employees, Users, service providers, unauthorized persons, etc.)
- The type of Health Data Breached
- HIE Participants likely impacted by Breach
- Number of individuals or records impacted/estimated to be impacted by the Breach
- Actions taken by Provider to mitigate the Breach
- Current Status of the Breach (under investigation or resolved)
- Corrective action taken and steps planned to be taken to prevent a similar Breach.

Provider shall have a duty to supplement the information contained in the notification as it becomes available and cooperate with other HIE Participants and HIE in performing such actions as are required by Applicable Law and as are necessary to mitigate the harmful effect of the Breach. If, on the basis of the notification, the HIE determines that (i) the other HIE Participants that have not been notified of the Breach would benefit from a summary of the notification or (ii) a summary of the notification to the other HIE Participants would enhance the security of the HIE or the HIE Participant's environment, it may provide, in a timely manner, a summary to such HIE Participants that does not identify any of the HIE Participants or individuals involved in the Breach. Provider, the HIE and effected HIE Participants shall decide on a case-by-case basis which party should notify any effected patients, and other parties as required by law.

HIPAA Business Associate Agreement

- The HIE is a Business Associate to each participant.
- Supports Protected Health Information (PHI) being sent to the ClinicalConnect HIE even if the patient has opted-out.
- Defines appropriate access to PHI, protection of PHI, accounting of PHI, and breach reporting.
- The HIPAA Business Associate Agreement must be agreed to without modification by each Participant.

Notice of Privacy Practices Addendum

- A one-page Notice of Privacy Practice Addendum has been developed that describes how ClinicalConnect manages and uses participants' PHI.
- The Notice of Privacy Practice Addendum must be included with each Participant's HIPAA Notice of Privacy Practices.
- The Notice of Privacy Practice Addendum must be used to without modification to the language by each Participant.