

Texas Health Services Authority Privacy and Security Task Force

July 27, 2011
10:00 am

Meeting Agenda

- Welcome and Announcements
- Overview and Discussion of Model Trust Agreement Elements
- Overview and Discussion of Health Information Security
- Future Meeting Schedule and Agenda Items
- Other Items?
- Adjournment

Privacy and Security Task Force Charter

This task force shall provide input on the development of privacy and security policies and standards that protect the privacy of patients involved in statewide HIE to the highest legal standard while enabling the secure exchange of health information. The task force will support ongoing analysis of a legal framework for the State of Texas.

Overview and Discussion of Model Trust Agreement

Elements of Trust Agreement

- **Parties** – Who should this include:
 - THSA, HIEs, White Space HISPs, THSA vendors for state level services, state agencies?
 - Others?
- **Proprietary Information** – Do the parties need to exchange any proprietary information other than PHI?
- **Network Operating Policies and Technical Requirements**– What should this include:
 - Interoperability standards?
 - Privacy and Security requirements?
 - Change procedures? Other?
- **Permitted Uses** – Should the agreement permit any disclosure that is authorized by law? What about disclosures to other states? How should the agreement account for differences in law that might be applicable to neighboring states?

Elements of Trust Agreement (cont.)

- **Prohibited Uses** – Who should get to determine when data from multiple sources can be aggregated and used for analytical purposes, or, if de-identified, for re-disclosure to third parties?
- **Damages** – Each party is responsible for their own actions. Should there be monetary penalties for breach above what is already provided by law? What if more than one party is responsible for a breach? Should there be a method to allocate responsibility among the responsible parties? Is this even possible?
- **Insurance** – How much and what types of insurance should each type of Participant and Vendor be required to maintain.
- **Indemnification** – Should the party who caused the harm have to defend and pay claims on behalf of another participant? What about when there are parties, such as state agencies, that cannot provide reciprocal indemnification?

Elements of Trust Agreement (cont.)

- **Termination** – Under what circumstances should a Participant be permitted to terminate participation in the exchange? Is there a wind-down period that is necessary to transfer information to other sources if a Participant decides to exit the network? If so, where should that information be transferred?
- **Archive/Escrow** – Is it necessary to have a third party escrow service maintain a back-up copy of PHI of a Participant in case the Participant is terminated and refuses to comply?
- **Survival** – What obligations should survive termination of or by a Participant?

“Implementing Privacy and Security Standards in Electronic Health Information Exchange ”

Patricia Gray, J.D., LL.M. Director of Research and External Affairs

University of Houston Health Law & Policy Institute

I. Overview On Implementing Privacy and Security Standards in Electronic Health Information Exchange

Key Points

- The HIPAA Privacy and Security Rules provide direction for policy makers to follow in working with those charged with the technical implementation of data security.
- The Privacy Rule addresses an individual's right to control use and disclosure of his or her protected health information (PHI).
- The Security Rule addresses the safeguards necessary to protect PHI from unauthorized access, use or disclosure.

II. The Security Rule

Key Points

- The Security Rule only applies to PHI that is created, received, maintained or transmitted in an electronic format (ePHI).
- A major goal of the Security Rule is to protect the privacy of patients' health data while giving covered entities the flexibility to implement the policies and procedures that are appropriate to address patient privacy.
- The key terms undergirding the Security Rule are confidentiality, integrity, and availability.

II. Security Rule (cont.)

Key Points

- The security safeguards are broadly categorized as administrative safeguards, physical safeguards, and technical safeguards.
- The security safeguards are supported by specific standards and implementation specifications.
- The security safeguard standards are defined as “addressable” or “required”.
- Covered entities are not permitted to consider cost, probability or criticality of potential risks to ePHI when deciding whether to implement a safeguard.

III. Security Rule Standards and Implementation Specifications

- Administrative, physical and technical safeguards are supported by a total of eighteen standards and thirty-six implementation specifications.
- Administrative safeguards encompass the policies and procedures to develop and maintain security measures to protect ePHI and to manage the conduct of workforce employees to protect ePHI.
- The Security Management Standard of the Administrative Safeguards is the foundation on which every covered entity's security activities are built.
- Physical safeguards are the measures, policies and procedures to protect electronic information systems from hazards and unauthorized intrusion.
- Technical safeguards are the policies and procedures to protect access to and control of ePHI.

IV. HIPAA Privacy Rule and Patient Rights

Key Points

- The Privacy Rule also implicates security of PHI in HIEs for patients' rights.
- The Privacy Rule encompasses all PHI whether it is being conveyed orally, in writing, or electronically.
- The Privacy Rule defines an individual's rights in relation to protection of his or her PHI.
- With limited exceptions, individuals have the right to access their own PHI, limit access to and disclosure of their data, obtain an accounting of the uses and disclosures of their data, and receive notice of a breach of access to their data.

V. Other Federal Provisions

Key Points

- The Clinical Laboratory Improvements Amendments of 1988 (CLIA) limit release of clinical laboratory reports to specifically authorized persons.
- The Red Flags Rule requires that entities protect patients against identity theft.
- The Federal Educational rights and Privacy Act (FERPA) implicates student health records maintained in public elementary and secondary schools.
- The Patient Safety and Quality Improvement Act authorizes review of both individual and aggregated patient data to improve patient safety.
- Federally funded substance abuse treatment programs have special requirements for accessing patient health information.
- The Veterans Health Administration requires written authorization from patients to release health information to non-VHA facilities.

Key Policy Questions

Implementing the Privacy and Security Rules

- What actions will demonstrate that covered entities have adequately complied with addressable standards for implementing the Security Rule?
- How will actions of business associates of covered entities be monitored and enforced for compliance with both the Security Rule and the Privacy Rule?
- How will HIEs ensure that patients and providers, as well as others who may have a role in the development of HIEs, understand and comply with the rights of patients?
- How will HIEs monitor the work of technical support workforce staff to ensure the privacy and security of patient health information?

Key Policy Questions (cont.)

Authenticating patient and user identification

- What entity will be responsible for authenticating health care providers? Health care plans? Health care clearinghouses?
- How will HIEs determine what limits, if any, should be placed on authenticated providers to access patient data?
- How will HIEs determine responsibility for maintaining audit trails?
- How will patient identification be verified? How will authenticated identification be maintained?

Key Policy Questions (cont.)

Ensuring accountability

- What policies are needed to manage requests for access to patient data?
- Research requests: How will HIEs manage requests for access to limited data sets that may include some patients' individually identifiable information? What steps to secure Institutional Review Board (IRB) approval will be required? How will risk assessments be reviewed?
- Emergency response: Under what circumstances will an HIE recognize a request from a disaster response coordinator such as the Red Cross? If a disaster declaration is required, may it be from the state or a local jurisdiction, or must it be a federal declaration?

Key Policy Questions (cont.)

Managing sensitive information

- What information will be classified as sensitive information?
- Will HIEs segment sensitive information? If so, what entity will be responsible for creating an electronic lockbox for securing sensitive information?
- How will HIEs secure “downstream” use of sensitive information if e-prescribing is used?

Key Policy Questions (cont.)

Consent and special populations

- How will HIEs manage consent and authorization issues related to those with diminished mental capacity or minors who have the right to accept or refuse certain treatment?
- How will HIEs extend minors' privacy rights as they relate to who can and cannot access their PHI, including an accounting for disclosure?
- How will HIEs manage access to sensitive information that a patient may wish to keep private, especially to the extent that such sensitive information may carry with it additional consent or authorization requirements?

Key Policy Questions (cont.)

Breach notification

- The rules related to breach notification focus on notice to the patient. However, other parties in an HIE network may also be impacted. How will breach notification be provided to other potentially affected parties in an HIE network?

Key Policy Questions (cont.)

Other

- Although Texas has a more expansive definition of covered entity than does HIPAA, an HIE could receive requests from entities that do not recognize Texas' definition. In addition, HIEs must manage requests from technical support organizations.
- How will HIEs respond to requests for access to patient health data by organizations and individuals who do not meet the definition of "covered entity" in order to ensure patients that their health data is both private and secure?
- What policies are needed to address requests from non-covered entities?
- Should HIEs be required to furnish their own notice of privacy practice?

Future Meetings:

- Wednesday, August 31
- Wednesday, October 5
- Wednesday, November 2
- Wednesday, November 30

Other items?

Steve Roddy - Associate Director of Policy & Planning
Jocelyn Dabeau – Legal & Policy Analyst
Texas Health Services Authority

(512) 814-0321

steve.rodny@thsa.org

jocelyn.dabeau@thsa.org

www.thsa.org