

Privacy and Security from a National Perspective

***Presentation to
2008 IMI Security Symposium***

Presenter:

Lisa A. Gallagher, BSEE, CISM, CPHIMS
HIMSS Senior Director, Privacy and Security

October 3, 2008

Overview

- **The Privacy and Security Landscape**
 - Background
 - Privacy and Security Challenges in the HC Information Sharing Environment
- **National Level Initiatives**
 - How they are addressing the P&S issues



Related Laws and Regulations

Privacy & Security Terminology

- **Health Information Privacy**
 - an individual's right to control the acquisition, uses or disclosures of their identifiable data
- **Confidentiality**
 - the obligation of those who receive the information to respect the privacy interests of those to whom the data relate
- **Security**
 - the physical, technical or administrative safeguards used to protect data from unwarranted access or disclosure
- **Use**
 - within an organization
- **Disclosure**
 - between/among independent organizations

Healthcare Challenges

- **Increased use of IT and web-based technologies**
- **Consumers are now becoming part of the healthcare model**
 - Existing paradigm for P&S (legal, regulatory and/or best practice) not adequate to address consumer involvement and awareness
- **Non-covered entities becoming part of the healthcare market**
 - Not covered by HIPAA; little regulation or guidance to follow
 - Potential trust issues that could endanger IT adoption
- **Secondary uses of data and data aggregation**
 - This is where privacy advocates make their case
- **Patchwork of Privacy legislation/regulation**

Health IT–Related Privacy Challenges

- Adoption of IT creates new challenges to safeguarding health privacy and confidentiality
- **Our overall challenge is to enable Health IT adoption is to establish requisite privacy policies and consumer protections in time to:**
 - Keep up with progress in technology and interoperability, etc.
 - Engender consumers' trust, and
 - Facilitate widespread adoption by consumers and providers.

Patient P&S Concerns

- **Types of information collected**
- **How the information is handled internally**
- **Whether and how information is disclosed to external parties** Children's privacy
- **Security policies and procedures: physical and transmission**
- **Data mining/analysis policies**
- **User access to information**
- **The ability to correct information that was recorded in error**
- **Ability for privacy options to opt-in or opt-out**
- **How a site notifies users about any changes**
- **How to contact a site with questions**

Most Visible P&S Topics

- **Accounting of Uses and Disclosures**
- **Data Ownership**
- **Patient (“Informed”) Consent**
- **Security Breach**
- **Secondary Uses of Health Data**

Privacy (and other) Concerns - EHRs

- **Security Features**
 - Support for Privacy Policies
- **Security Vulnerabilities**
- **“George Clooney” Disclosures**

Privacy (and other) Concerns - PHRs

HIMSS defines an ePHR as follows: An electronic Personal Health Record (“ePHR”) is a universally accessible, layperson comprehensible, lifelong tool for managing relevant health information, promoting health maintenance and assisting with chronic disease management via an interactive, common data set of electronic health information and e-health tools. The ePHR is owned, managed and shared by the individual or their legal proxy(s) and must be secure to protect the privacy and confidentiality of the health information it contains. It is not a legal record unless so defined and is subject to various legal limitations.

Privacy Concerns:

- **Data Sharing/Secondary Uses**
- **Data aggregation**
- **Patient control**
- **Provider responsibility to push data?**
- **Varying Implementation models**
 - **“PHR-like” services**

Privacy (and other) Concerns - RHIOs/HIEs

- **Legal/Regulatory**
 - State and Federal Privacy Laws – existing and proposed
 - Complexity/time of cross-organizational agreements
- **Liability/Security**
 - “There were real legal concerns from some of the other entities [in the exchange] about the liability of having data fall into the wrong hands, despite all we had done in the way of security.”
- **Cost of implementing Privacy Policy**
 - concerns about the possible expense of building the filters needed to sift sensitive information from the data stream before it was transmitted to other members of the exchange
- **Cost of Operations/Business Model, esp. for 501(c)3**

HHS - Office of the National Coordinator (ONC)

- Serves as the Secretary's principal advisor on the development, application, and use of health information technology
- Coordinates the Department of Health and Human Services' (HHS) health information technology policies and programs internally and with other relevant executive branch agencies
- Develops, maintains, and directs the implementation of HHS' strategic plan to guide the nationwide implementation of interoperable health information technology in both the public and private health care sectors, to the extent permitted by law
- Provides comments and advice at the request of OMB regarding specific Federal health information technology programs.

Relevant National Level Initiatives

What part are they playing relating to privacy/security?

- **Nationwide Health Information Network (NHIN)**
 - 4 prototype contractors
 - addressed security solutions
- **NHIN Collaborative Demonstrations**
 - HHS recently awarded contracts to multiple health information exchanges to begin trials for the NHIN
 - Will test and demonstrate the exchange of private and secure health information among providers, patients and other stakeholders.
 - The HIEs also will adopt scenarios designated as priorities by the American Health Information Community (AHIC), an HHS advisory committee.

NHIN Demonstrations (cont.)

#1 Emergency Care Scenario:

- Regenstrief Institute: Marc Overhage, MD, PhD
- HealthLINC-HealthBridge: Todd Rowland, MD
- Indiana Network for Patient Care (INPC)
- Others that were mentioned in this scenario but not necessarily part of the demo included

#2. Transfer of Care Scenario

- Lovelace Clinic Foundation & New Mexico HIE: Robert White, MD, MPH
- New Mexico Health Information Collaborative
- Long Beach Network for Health: Paul Fu, Jr., MD, MPH

#3: Wounded Warrior Scenario

- VA: Linda Fischetti, RN and Vinod Krishnan, MD
- DOD: Steve Steffensen, MD
- Kaiser Permanente: George Peredy, MD
- Other participants that were mentioned & participated included:
- MedVirginia
- CareSpark
- NCHICA

AHIC/AHIC CPS WG

- AHIC - federal advisory body, est. in 2005 to make recommendations to the Secretary of the U.S. Department of Health and Human Services on how to accelerate the development and adoption of health information technology.
- AHIC Successor – a public-private partnership to succeed the initial federal advisory committee.
- AHIC Confidentiality Privacy Security WG – Final recommendations letter to AHIC regarding policy issues, challenges, and considerations for protecting electronic PHI, including:
 - Policies regarding Network Access
 - Policies regarding a Network's Own Activities
 - De-identification
 - Consistent Rules for Personal Health Information
 - Roles, Rights and Responsibilities of Consumers
 - Safeguarding Information in a Personal Health Record

Relevant National Level Initiatives (cont.)

What part are they playing relating to privacy/security?

- **Certification Commission for Health Information Technology (CCHIT)**
 - Established requirements for Functionality, Interoperability and **Security** Features in EHR products
 - Potential certification of PHRs:
 - Interoperability
 - Portability
 - Security features
 - *Not* functionality

Relevant National Level Initiatives (cont.)

What part are they playing relating to privacy/security?

Health Information Technology Standards Panel (HITSP)

The mission of the Healthcare Information Technology Standards Panel is to serve as a cooperative partnership between the public and private sectors for the purpose of achieving a widely accepted and useful set of standards specifically to enable and support widespread interoperability among healthcare software applications, as they will interact in a local, regional and national health information network for the United States.

Focus areas for Interoperability Specifications:

- Biosurveillance
- Consumer Empowerment
- EHR
- etc.
- ***Privacy and Security***

Other Relevant National Level Initiatives (cont.)

Health Information Security and Privacy Collaboration (HISPC)

- Tremendous variation in:
 - Practice and policy
 - Interpretation of regulations (e.g., HIPAA and 42CFR Part 2)
 - Laws (e.g., CLIA, FERPA, ERISA)
 - Application of Minimum Nec Std
- Lack of Trust
 - Between organizations (e.g., HIEs)
 - Consumers
 - Providers
- Cultural and Business Issues
 - Concerns about Liability
 - Questions about who “owns” the data
 - Resistance to change
- Burden
 - Financial
 - Workflow
- Other
 - Lack of ability to match patient records
 - Lack of existing audit programs
 - Role-based access control – lack of way to segregate data poses challenges
 - Lack of standard authentication and authorization protocols

HISPC Project Materials:

<http://www.rti.org/page.cfm?objectid=09E8D494-C491-42FC-BA13EAD1217245C0>

HISPC - Final Report Recommendations

State-level

- Practice and Policy
 - Interpreting HIPAA privacy rule
 - Uniform consent
- Legal and Regulatory
 - State laws – finding and interpreting and application to HIE
 - Intersection with federal law
- Technology and Standards
 - Data security; four As: authentication, authorization, access and audit
 - Transmission
 - Patient identity management
 - Segmenting data
- Education
- Implementation of Governance of Solutions

National Level

- National standards
- Clarifications/revisions to federal regulations
- Funding

Existing Laws Affecting the Industry

“Current federal and state laws regulating the flow of health information are a complex and confusing patchwork.” – Markle 2004

- **HIPAA Regulations** - apply (only) to “covered entities”
 - health plans, health care clearinghouses, and health care providers that engage in electronic transactions for which HIPAA standards have been adopted
- Many other types of entities maintain or obtain medical information, but are not subject to HIPAA regulations
 - employers, certain types of insurers, and providers that do not engage in electronic transactions

Other Laws and Regulations

“...Only to individually identifiable health information held or maintained by a covered entity or its business associate acting for the covered entity....Health information that is held by anyone other than a covered entity, including an independent researcher who is not a covered entity, is not protected by the Privacy Rule and may be used or disclosed without regard to the Privacy Rule. There may, however, be other Federal and State protections covering the information held by these entities that limit its use or disclosure.”

(NIH Guidance, 4/15/03)

- Federal Privacy Act
- Federal Trade Commission Act
- Gramm Leach Bliley
- Sarbanes Oxley
- 42CFR Part 2 – Confidentiality of Alcohol and Drug Abuse Patient Records Rule
- Other Laws (e.g., CLIA, FERPA, ERISA)
- PCI Security Standard

State Laws, Regulations, etc.

- **State laws vary with respect to use and disclosure (HISPC)**
- **“Program-specific” requirements**
- **“Special conditions for Sensitive Health Information”**
- **Specific privacy *exceptions* for certain health information**
- **Around 39 states require disclosure of security breaches related to HIT. In these states, notification of affected individuals as well as law enforcement is required when unauthorized acquisition or access to personal information occurs**
- **At least one state (WA) has passed legislation that has mandated security:**

“A healthcare provider shall affect reasonable safeguards for the security of all health information it maintains. Reasonable safeguards shall include affirmative action to delete outdated and incorrect facsimile transmission or other telephone transmittal numbers from computer, facsimile, or other databases. When health care information is transmitted electronically to a recipient who is not regularly transmitted health care information from the health care provider, the health care provider shall verify that the number is accurate prior to transmission”. [\[1\]](#)

HIPAA vs. State Laws

- State laws present significant challenge
 - May be more stringent
 - Vary from State to State and/or address Multi-state issues (RHIOs)
 - Authorization requirements may vary
 - State laws and regulations found in many places/types
 - Reqs likely to vary with type of data (mental health, AIDS/HIV, substance abuse (there are federal reqs too!))

Recent National Level Legislative Activity - 110th Congress

- **Wired for Health Care Quality Act (S.1693, HR.3800)**
- **The Technologies for Restoring User's Security and Trust in Health Information Act of 2008 ("TRUST" Act) (HR.5442)**
- **The Health Information Privacy and Security Act (S.1814)**
- **Independent Health Record Trust Act (HR.2991)**
- **PRO(TECH)T Act (HR.6357)**
- **Health-e Information Technology Act (HR.6898)**

A Snapshot...

Privacy Topic	S.1693 - "Wired Act"	H.R.6357 - "PRO(TECH)T Act"	H.R.6898 - "Health-e IT", "Stark"
Business Associates			
	When contracting with a third party service provider, including those in a foreign country, entities must take reasonable steps to ensure third party is capable of maintaining security and privacy of PHI and require such steps via contract. This provision is effective 30 days after the Secretary has finalized guidance for compliance with this provision. §3016	Applies HIPAA Security Rule requirements for administrative, physical, and technical security safeguards to business associates and subjects them to the same potential civil and criminal penalties for failure to comply. §301(1)-(2)	Applies HIPAA Security Rule requirements for administrative, physical, and technical security safeguards and any new HIT security standards adopted by HHS under Title I to business associates and subjects them to the same potential civil and criminal penalties for failure to comply. §401(1)-(2)

Privacy Topic	S.1693 - "Wired Act"	H.R.6357 - "PRO(TECH)T Act"	H.R.6898 - "Health-e IT", "Stark"
Security Breach			
Security Breach	The Secretary shall include exemptions to standards for law enforcement and national security purposes.	Must notify each individual whose information is or reasonably believed to have been accessed, acquired, or disclosed as a result. §302(a)	Must notify each individual whose information is or reasonably believed to have been accessed, acquired, or disclosed as a result. §402(a)
		Business associates must notify a covered entity of any breaches that occur, including details regarding affected or possibly affected individuals. §302(b)	Business associates must notify a covered entity of any breaches that occur, including details regarding affected or possibly affected individuals. §402(b)

Privacy Topic	S.1693 - "Wired Act"	H.R.6357 - "PRO(TECH)T Act"	H.R.6898 - "Health-e IT", "Stark"
Accounting of Disclosures		<p>In addition to accounting for all nonroutine disclosures as required under HIPAA, a covered entity that uses or maintains an EMR must account for all non-oral disclosures related to TPO for a period of 3 years.</p> <p>§312(c)(1)</p> <ul style="list-style-type: none"> • An EMR is defined as "an electronic record of individually identifiable health information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff within a single organization." <p>§312(c)(2)</p>	<p>In addition to accounting for all nonroutine disclosures as required under HIPAA, a covered entity must account for all non-oral disclosures of PHI used or maintained in an EHR or EMR related to TPO for a period of 3 years.</p> <p>§405(c)(1)</p> <ul style="list-style-type: none"> • An EHR is defined as "an electronic record of health related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff of one or more organizations that conforms to [HIT standards adopted in this Act] and is made accessible electronically to other health care organizations and authorized users." <p>§400(5)</p> <ul style="list-style-type: none"> • An EMR is defined as "an electronic record of individually identifiable health information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff within a single organization." <p>§400(6)</p>

Questions?

Lisa A. Gallagher, BSEE, CISM, CPHIMS
Senior Director, Privacy and Security
703-581-2014
lgallagher@himss.org