

Privacy and Security Overview

*Presentation to
HIMSS Louisiana Chapter
by*

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

October 26, 2007

Overview

- The Privacy and Security Landscape
 - Privacy and Security Challenges in the Information Sharing Environment
 - National Level Initiatives
 - How they are addressing the issues
 - How HIMSS contributes
 - *Hot* 🔥 P&S Topics
- Appendix: HIMSS P&S Initiatives

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 real challenge 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 of any kind
- 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

Relevant National Level Initiatives

What part are they playing relating to privacy/security?

How does HIMSS contribute?

- **NHIN Prototypes**
 - 4 prototype contractors address security solutions
 - **HIMSS provided public comments on requirements; attended conferences**
- **NHIN Implementation Contract Awards**
 - HHS recently awarded \$22.5 million to nine health information exchanges to begin trials for the NHIN
 - 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, an HHS advisory committee.

Relevant National Level Initiatives (cont.)

What part are they playing relating to privacy/security?

How does HIMSS contribute?

- **CCHIT**
 - Established requirements for Security Features in products
 - Now discussing in terminology of privacy (ref: recent AHIC testimony)
 - However, there is recognition that ensuring security features does not completely solve the privacy issues
 - Recent *vulnerability assessment** by third party
 - Potential certification of PHRs:
 - Interoperability
 - Portability
 - Security features
 - *Not* functionality
 - **HIMSS provides public comments consolidated from many SCs**
 - **HIMSS provides technical support**
 - **Lisa Gallagher member of Security Expert Panel**

Relevant National Level Initiatives (cont.)

What part are they playing relating to privacy/security?

How does HIMSS contribute?

- **HITSP – Standards Harmonization**

- Focus areas for Interoperability Specifications:**

- Biosurveillance
 - Consumer Empowerment
 - EHR
 - Privacy and Security
 - **HIMSS has members on the WG**
 - Current discussion –
 - **policy framework under which to create technical standards**

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>

Privacy (and other) Concerns - EHRs

- **Security Vulnerabilities**
 - see Hot Topics
- **Support for Privacy Policies**
- **“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.

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

Privacy (and other) Concerns - RHIOs

- Failure of The Santa Barbara County (CA) Care Data Exchange
 - Legal/Regulatory
 - **did the care model exchange meet state privacy laws/other regs?**
 - **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

Considerations for HIEs

- Degree of adoption of HIE
- Health care market forces in state
- Legal and regulatory conditions related to health information
- Demographic composition of the state
- Financial status of the state
- Cultural and historical characteristics

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

HISPC – moving forward

- State team subcontracts have been extended through December 2007 to implement a foundational component of their plan
- Moving toward multi-state and regional coordination and collaboration
 - HISPC state project leaders have met with the State Alliance for eHealth Health Information Protection Taskforce
 - Forming multi-state and regional collaborative work groups that will continue the work beyond the end of this contract
 - Representatives from all 56 states and territories have been invited to participate in those work groups
- The state teams will come together for a National Meeting on November 1-2, 2007 in DC.

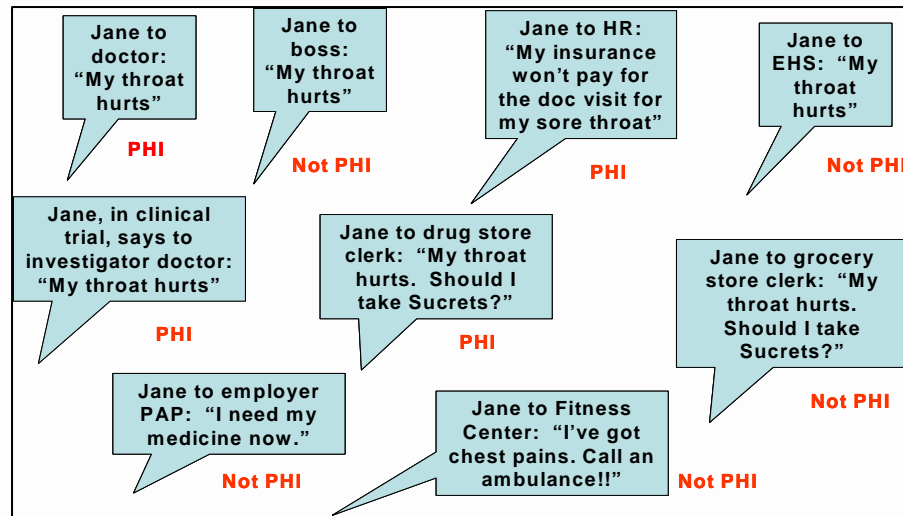
Where does the law stand on these issues?

“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

HIPAA – Allowed Disclosures

- HIPAA – law is provider/institution-focused
- PHI, as defined by HIPAA, is *context-specific*



Doug Peddicord, PhD

"...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."

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
- At least six states (AZ, MA, MI, RI, VA, VT) 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

HIPAA vs. State Laws

- State laws present significant challenge
 - May be more stringent
 - Vary from State to State (Multi-state 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 reqts too!))

Model Data Use Agreements

- http://www.connectingforhealth.org/commonframework/docs/M2_ModelContract.pdf
- <http://www.volunteer-ehealth.org/news/info/2006/09/midsouth-ehealth-alliance-data-sharing.php>
- <http://www.mahealthdata.org/data/DataUseAgreement.pdf>
- <http://www.academyhealth.org/privacy/tools.pdf>

Hot Privacy and Security Topics

- **“Study Concludes EHR Security at Risk”**
www.ehvrp.org
http://www.ehvrp.org/images/07_09_17_FINAL_eHVRP_releases_study_results.pdf
- **NCVHS Study - Secondary Uses** www.ncvhs.hhs.gov
 - Federal Privacy Legislation
 - Modifications to HIPAA
 - Data Stewardship Principles
 - Health Data Use Risk/Benefit Analysis Framework
- **Press Release by Patient Privacy Coalition**
- **Privacy Framework - ONC**

Questions?

Lisa A. Gallagher, BSEE, CISM
Senior Director, Privacy and Security
703-562-8816 (VA office)
lgallagher@himss.org

Appendix

- HIMSS Privacy and Security Initiatives

Privacy and Security Committees and Work Groups

HIMSS is dedicated to strengthening its Privacy and Security Initiative by continuing to work with providers, practice managers, and communities to identify and demonstrate Privacy and Security issues and solutions.

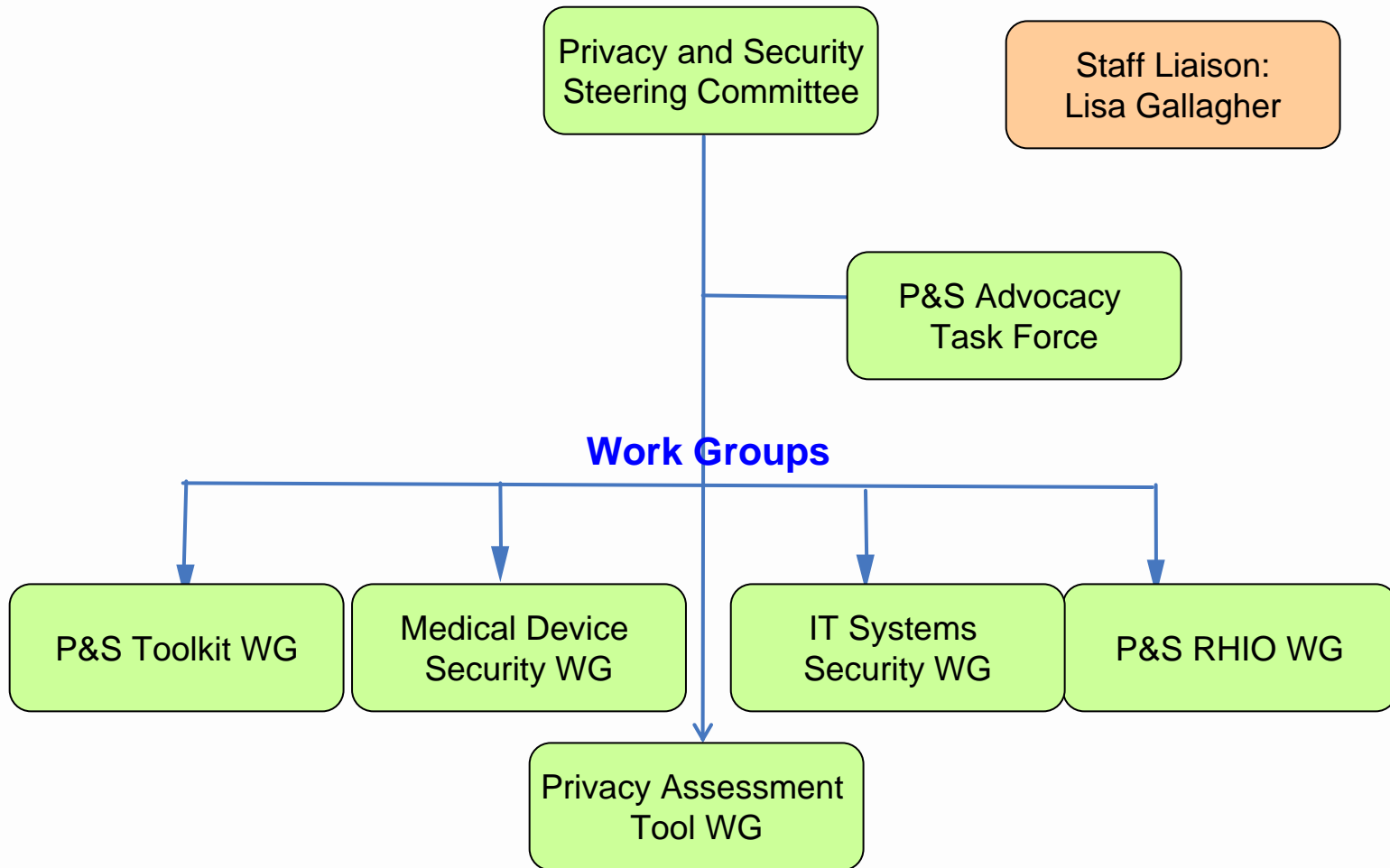
Staff Leadership:

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

Privacy and Security Steering Committee:

Chair - Barbara Demster MS, RHIA, CHCQM
Chief Compliance & Privacy Officer
Benchmark Consulting Services Inc

HIMSS FY08 Privacy and Security Committee Structure



P&S Steering Committee

Chairperson:

Barbara Demster MS, RHIA, CHCQM

Purpose/Goal:

By 2014, all entities who use, send, or store health information meet requirements for confidentiality, integrity, availability and accountability based on sound risk management practices using recognized standards and protocols.

P&S Toolkit WG

Chairperson:
Ted Cooper, MD

Purpose:

Ongoing maintenance and updates to the **HIMSS Privacy & Security Toolkit** which outlines general principles and provides best practices and examples of how health care providers should manage the security of their paper and electronic records.

<http://www.himss.org/ASP/privacySecurityTree.asp?faid=78&tid=4>

Medical Device Security Work Group

Chair Person:
Frankie Rios

Purpose:

Identify both the security issues associated with medical devices and systems, and the best practices available to address those issues.

Work Product: MDS² Disclosure Form

*Manufacturer Disclosure Statement for Medical Device Security (MDS²)

Information Systems Security WG

Chairperson: Mac McMillan

Purpose:

The Information Systems Security WG is dedicated to creating a framework for achieving an integrated information security system model for healthcare as well as creating practical best practice guides and tools for healthcare information security practitioners that individual security managers can use to assist them in:

- developing their own programs,
- guiding their product selection processes, and
- informing their policy decisions.

P&S RHIO Work Group

Chairperson:

J. William Woloszyn, RHIA, CHPS

Purpose:

The purpose of the HIMSS Work Group is to investigate and develop thorough documentation that will provide RHIO privacy and security guidelines providing protections that meet or exceed minimum requirements set by regulations.

Privacy Impact Assessment WG

Chairperson: Mariann Yeager, MBA

Purpose:

The purpose of the HIMSS Privacy Impact Assessment Work Group is to investigate and determine the feasibility of the development of a Privacy Impact Assessment Tool, designed to document/describe the personal and clinical information flows via inpatient and outpatient systems and analyze the possible privacy impacts that the information flows may have on the privacy of individuals.

P&S Advocacy Task Force

Purpose:

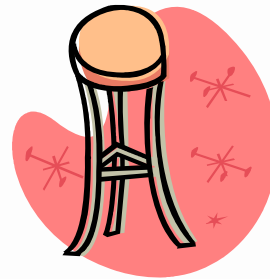
Support HIMSS Members and HIMSS Advocacy activities:

- Developed P&S Legislative Principles
- Articulate HIMSS positions on regulatory issues
- Support Advocacy Education activities

Future Work Product: Model P&S legislative language

Need to balance:

- Technology/Standards
- Policies
- Trust



Challenges:

- National-level discussion on policy issues
- Linking of technology and policy efforts
- Not impeding the adoption of Health IT
- Education of consumer/patient to engender “trust”