Privacy and Security Concerns with EHRs and PHRs

Prepared by:
Lisa A. Gallagher
Director, Privacy and Security

Prepared for:
Project HITCh Meeting
February 27, 2007

Topics

• Privacy and Security Background
• Related Work at the National/State Level
• Privacy Policy Topics
• Implementation Topics
Terminology

• Health Information Privacy
  – An individual's right to control the acquisition, uses or disclosures of their identifiable data

• Security
  – the physical, technical or administrative safeguards used to protect data from unwarranted access or disclosure

• Confidentiality
  – the obligation of those who receive the information to respect the privacy interests of those to whom the data relate

Who do Patients “Trust”?*

In descending order, the most trusted sources of information were*:

• providers supplying information and administering PHRs,
• insurance carriers,
• government agencies
• third-party vendors
• The least trusted were employers

*BCBS survey
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

AARP, “Personal Health Records: An Overview of What is Available to the Public”

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”
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

Text excerpted and paraphrased from the testimony of Susan McAndrew, DHHS/Office of Civil Rights to the AHIC Consumer Empowerment WG

HIPAA (cont.)

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

“…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)
HIPAA and EHRs/PHRs

- EHRs - Most are covered by HIPAA
- PHRs
  - NOT ALL PHR scenarios are covered by HIPAA
  - SOME ARE
  - In any case, patients should be able to expect that privacy security protections consistent with the HIPAA Security Rule be implemented:\(^1\):
    - Entities not covered by HIPAA that offer PHR systems should voluntarily adopt strict privacy policies and practices and should provide clear advance notice to consumers of these policies and practices, including a full description of all uses of PHR data
    - No health information in a PHR be used without the express consent of the consumer, which may be obtained in conjunction with the notice

PHR Examples – Covered or Not?

- **Physician practice** makes PHR product available to patient. PHR product is hosted by physician practice or vendor.  
  - Covered by HIPAA

- **Health Plan (Payer)** offers patient portal to enrollees, patient accesses portal through Plan website. Portal hosted by plan or third-party hosting provider.  
  - Covered by HIPAA

- **Patient selects PHR** product based on features, and not in conjunction with specific care provider. Product is web-based and patient determines access to data.  
  - Not covered by HIPAA

- **Employer** offers employee portal for wellness management, etc. Patient accesses portal through Plan website. Portal hosted by plan or third-party hosting provider.  
  - Not covered by HIPAA

---

\(^1\) – NCVHS recommendations in letter to DHHS Secretary, dated Sept 9, 2005
What was the issue again?

• Turns out, it may not be just “Privacy and Security”
• It is about who accesses, who owns, and who controls the information stored in a PHR, and how that information might be used/exchanged
• Privacy policies and security features can be defined from there
• At the same time, any measures that we implement must acknowledge and support the requirement of healthcare providers for timely access to accurate and complete health information in treating individuals who seek their care.¹

“The government’s greatest challenge is not finding the right technology or creating the most sophisticated technical infrastructure – it is finding agreement on the complex array of policies necessary for trustworthy information exchange”

-Dr. Carol Diamond, Markle Foundation

Privacy Policy Topics

• **Non-covered entities** – collection and use of health data by entities not covered by HIPAA
• **Secondary uses of data** – non direct-care use of health data, including but not limited to analysis, research, quality and safety measurement and other business including strictly commercial uses¹.
• “**Opt-in**” or “**Opt-out**” – patient determination of whether their health data should be part of the NHIN or other HIE
• **Minimum Necessary** (i.e., Use Limitation) – data only be used for the stated purpose
• **Other Federal Laws** – Privacy Act, Consumer Protection Laws, etc.
• **Differing State Laws** – HISPC study out soon
• **International Laws** – UK, EU, Australia²

Implementation Topics

• Architecture
  – Federated
  – Centralized
  – Hybrid

• Technical
  – Master Patient Index – including patient identification algorithms to facilitate accurate exchange of information
  – PKI – to mediate data access across HIE
  – Common record format – facilitates information exchange
  – Uniform vocabulary – facilitates information exchange
  – Encryption – to secure data in transit
  – Identity Proofing – in-person, technical, etc.
  – Digital Signatures – to secure data in transit
  – Authentication – biometrics, etc.
  – Access controls - role based, context-based, etc.
  – Audit – record of accesses

Contact Information

Lisa A. Gallagher, BSEE, CISM
Director, Privacy and Security
lgallagher@himss.org
703-837-9817 - office
703-581-2014 - mobile
Appendix

Background Information on Privacy Concepts and work being done at National and State Level

Markle Principles

Consists of nine guiding principles, providing a multi-layered approach to ensuring confidentiality of patient data in an information-sharing system or network. These principles are:

1. Openness and Transparency
2. Purpose Specification and Minimization
3. Collection Limitation
4. Use Limitation
5. Individual Participation and Control
6. Data Integrity and Quality
7. Security Safeguards and Controls
8. Accountability and Oversight
9. Remedies

Recommendations

• These recommendations cover several topics central to the challenges for safeguarding health privacy in the NHIN environment:
  – the role of individuals in making decisions about the use of their personal health information,
  – policies for controlling disclosures across the NHIN,
  – regulatory issues such as jurisdiction and enforcement,
  – use of information by non-health care entities, and
  – establishing and maintaining the public trust that is necessary to ensure the NHIN is a success.

AHIC Consumer Empowerment Guiding Principles

• Individuals should be guaranteed the right to access their own health information
• Individuals should be able to access their PHII conveniently and affordably
• Individuals should how their PHII may be used and who has access to it
• Individuals should have control over whether and how their PHII is shared
• Systems for electronic health data exchange must protect the integrity, security, privacy and confidentiality of an individuals information
• The governance and administration of electronic health data exchange networks should be transparent and publicly accountable
Charge of AHIC CPS WG

Broad Charge for the Workgroup:
• Make recommendations to the Community regarding the protection of personal health information in order to secure trust, and support appropriate interoperable electronic health information exchange.

Specific Charge for the Workgroup:
• Make actionable confidentiality, privacy, and security recommendations to the Community on specific policies that best balance the needs between appropriate information protection and access to support, and accelerate the implementation of the consumer empowerment, chronic care, and electronic health record related breakthroughs.

Other Relevant National Level Initiatives

• NHIN – 4 prototype contractors address security solutions
• CCHIT – Establish Requirements for Security Features in products
• HITSP – Standards Harmonization
  – Focus areas for Interoperability Specifications:
    • Biosurveillance
    • Consumer Empowerment
    • EHR
    • Privacy and Security – NEW
• Health Information Security and Privacy Collaboration (HISPC)
  – identify variations in privacy and security practices and laws affecting electronic health information exchange,