HIPAA Privacy & Security: IT Challenges

Harvard Colloquium
August 21, 2001

Tom Hanks
Director Client Services
(312) 701-2466
Tom.Hanks@us.pwcglobal.com

Working Together: HIPAA Security and Privacy

- **Security NPRM - 1998**
- **Privacy Rule – final 4/14/2001**
- **Privacy Guidelines 7/6/2001**
- **Final Security rule will be harmonized with the final Privacy rule**
- **Final Privacy rule provides guidance for the final Security rule**

Security IT Challenges

- Audit trails
- Authentication
- Access control
- Encryption over open networks
  - Email

Security – Safeguarding PHI

- **Establish and maintain *reasonable* and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and *availability* of the information**

Security – Safeguarding PHI (cont'd)

- No proscribed implementation
- Reasonably required to protect from intentional or unintentional violation
- Each health care business determines their own needs
- Implementation varies according to size and type of entity
- Must consider cost

Security – Safeguarding PHI (cont'd)

- **Requirements are technology neutral - - each organization determines the technology to achieve outcome**

Privacy IT Challenges

- **Accounting for disclosure**
- **Audit trail**
- **Amendments to the medical record**
- **Authentication**
- **Access controls – granularity of role-based access control**

Privacy – Safeguarding PHI

- **Must have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI**
- ***Reasonably*** **safeguard health information**

Privacy – Guide to Security

- Final Privacy rule gives us guidance on what to expect from final Security Rule
- Both Security and Privacy address safeguarding health information
- No material changes to Security NPRM expected
- Final Security rule is being aligned with final Privacy rule

Privacy – Safeguarding PHI - Reasonably?

- Scalability of requirements
- Minimum necessary –
  - Role-based access controls
- Internal use & disclosure
- Accounting for Disclosures
- What kind of “safeguards” are required

Privacy – Safeguarding PHI - Reasonably? (Cont'd)

- Common sense, flexible and scalable
- Implementation varies with size and type of activities
- Must consider cost
  - Strike a balance between protecting privacy and cost

Privacy – Safeguarding PHI - Reasonably? (Cont'd)

- **Not required to guarantee the safety of PHI against all threats**
- **Theft of PHI may not be a violation if reasonable policies in place**

Privacy - Minimum Necessary Provision

Except for treatment…

- **Disclosure of any patient information is limited to the minimum amount necessary to accomplish the purpose of the disclosure**
- **Internal & external**

Privacy – Access Controls

- **Privacy rule establishes role-based access policies**
- **Identify persons or class of persons that need access to PHI**
- **Limit access to only the PHI needed to perform their job**

Privacy – Access Controls Reasonable Efforts

- Takes into account the ability of the entity's existing computer system
- Practicality of organizing systems to allow this capacity
- Recognizes limitations on parsing paper records

Security – Audit Trails

- **Audit trails required – no implementation provision**
- **The data collected and potentially use to facilitate a security audit**
- **Internal audit requirement to review records of system activity – audit trail**

Privacy – Defines Audit Trail Expectations

- **Audit trails do not usually record each time a record is used or reviewed**
- **Audit trails typically record each time a sensitive record is altered**
- **Important to coordinate Accounting for Disclosure with Audit Trails in Security**

Privacy – Accounting for Disclosure – Not an Audit Trail

- Date of each disclosure
- Name and address, if known, of person or entity receiving the PHI
- Brief description of information disclosed
- Purpose for disclosure or copy of individual's authorization

Privacy Guidelines – Reasonable?

Encryption not required for:

- **Wireless or other emergency medical radio communications**
- **Telephone systems**

Privacy Guidelines – Reasonable? (Cont'd)

- **"The rule does not require that all risk be eliminated…"**
- **"Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information."**

Privacy Guidelines – Reasonable? (Cont'd)

In limiting access, covered entities are NOT required to completely restructure existing workflow systems, including… upgrades of computer systems, in order to comply with the minimum necessary requirements

Privacy Guidelines – Reasonable? (Cont'd)

Patient Care Retains Primacy

"In determining what is reasonable, the Department will take into account the concerns of covered entities regarding potential effects on patient care and financial burden."

Thank you!