

Current State of Healthcare IT Security

Joseph W. Hales, PhD

September 10, 2008



Privacy

- “an individual's desire to limit the disclosure of personal information”
- fundamental right to control the dissemination and use of information
 - information disclosed may be used to harm his or her interests

For the Record. National Academies Press, 1997



Confidentiality

a condition in which information is shared or released in a controlled manner

For the Record. National Academies Press, 1997



Security

measures that organizations implement to protect information and systems from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss

- Confidentiality
- Integrity
- Access

For the Record. National Academies Press, 1997



Security Plan Basics

- Access Control
- Authentication
- Authorization
- Audit
- Availability
- Backup and Recovery
- Administration
 - Policy & Practices
- Authenticity/Integrity
- Attributability
- Non-repudiation

What Are We Protecting?

- Medical Record
 - Paper/electronic
 - Inpatient/outpatient
 - Business artifacts (e.g., claims)
 - Encounter/data
 - Email

For the Record. National Academies Press, 1997



What Are We Protecting?

- Identity
- Business operations
- Intellectual property
- Physical assets



From (or For) Whom

- Hackers
- Scammers
- Idiots
- Nature
- Terrorists
- Users
- Customers
- Regulators
- Attorneys

From (or For) Whom?

- Patient
- Primary Care MD
- Consulting MD
- Health Insurance Co.
- Clinical Laboratory
- Local Retail Pharmacy
- PBM
- Local Hospital
- State Bureau of Vital Statistics
- Accrediting Org.
- Employer
- Life Insurance Co.
- Medical Information Bureau
- State Public Health
- Researcher

HIPAA

Health Insurance Portability and Accountability Act of 1996

- Really about health insurance
- Electronic Transactions
- National Provider Identifier
- Privacy and Security

HIPAA Privacy

Standards for Privacy of Individually Identifiable Health Information (45 CFR Part 164.5xx)

- PHI – protected health information
- Minimum necessary
- Treatment, payment and health care operations (TPO)
- De-identification
- Notice of Privacy Practices
- Criminal and civil penalties



HIPAA Security

Security Standards for the Protection of Electronic Protected Health Information (45 CFR Part 164.3xx)

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational requirements
- Policies and procedures, documentation



HIPAA Event Timeline

- January 2006 – Providence Health System, Portland OR
 - Loss of 10 computer disks; 365,000 patients
- March 2007 – Piedmont Hospital, Atlanta GA
 - First (reported) OIG HIPAA (security) audit
- January 2008 – CMS
 - PriceWaterhouseCoopers to conduct 10-20 on-site HIPAA security inspections annually



HIPAA Event Timeline (continued)

- April 2008 – NY Presbyterian Hospital, NYC NY
 - Employee charged with selling records; 50,000 patients
- June 2008 – University of Utah, Salt Lake City UT
 - Loss of backup tapes; 2.2 million patients
- July 2008 – Providence Health System
 - Fined \$100,000 for HIPAA violation



HIPAA Event Timeline (continued)

- July 2008
 - 981 Privacy complaints (38,204 to date)
 - 25% require investigation (historical)
 - 2/3 (18% of total) require corrective action
 - 1/3 do not uncover a violation
 - OCR has not imposed a civil penalty in five years

Health Information Privacy/Security Alert <http://www.melamedia.com/HIPAA.Stats.home.html>



SOX

Sarbanes-Oxley Act of 2002

(Public Company Accounting Reform and Investor Protection Act of 2002)

- Internal controls
 - Certification
 - Assessment
- Documentation
- Retention and e-discovery



PCI

Payment Card Industry Data Security Standards

A company processing, storing, or transmitting payment card data must be PCI DSS compliant

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an Information Security Policy



Breach Laws

- State laws governing the loss or theft of personally identifiable information
(Utah Code: 13-44-101, -102, -201, - 202, -310)
 - Record destruction requirements
 - Disclosure requirements



110th Congress

Senate

- S 1693 (HR 3800) Wired for Healthcare Quality Act
- S 1814 Health Information Privacy and Security Act



110th Congress

House of Representatives

- HR 493 Genetic Information Nondiscrimination Act of 2008 (SIGNED 5/21/2008)
- HR 2991 Independent Health Record Trust Act of 2007
- HR 3800 (S 1693) Promoting Health Information Technology Act
- HR 5442 "TRUST" in Health Information Act of 2008



Personal Health Records

- Provider controlled (MyHealth)
- Patient controlled (WebMD)
- Hybrid (Dossia)
- Platform (HealthVault)



Public Perception of EHR

- Wall Street Journal/Harris Interactive (Nov. 2007)
 - 75% - patients receive better care
 - 63% - reduce medical errors
 - 55% - reduce medical costs
 - 50% - patient privacy more difficult to ensure
 - (down from 61% in 2006)



Threats

- Natural Disaster
- Negligence
- Intruder
 - External media
 - Compromised websites
 - E-mail



Summary

- Fundamentals
- Compliance burden
- Policy debate continues

