In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information

Sharona Hoffman

Case Western Reserve University

Who wants PHI?

- Employers
- Lenders
- Drug companies
- Advertisers & marketers
- Insurers
- Educational institutions
- Blackmailers
- Romantic partners

Confidentiality is often violated

- Computers are sold without removal of PHI from hard drives
- Hackers
- Banker who served on state health commission called in loans of cancer patients
- Computers are stolen

HIPAA Security Rule (2005)

Delineates administrative, physical and technical safeguards

- PHI – individually identifiable health information that is electronically or otherwise transmitted or maintained
- Rule applies to health plans, health care clearinghouses, and health care providers who transmit health information electronically for billing and claims purposes

Administrative Safeguards

- Standards: security management processes, workforce security, information access management, security awareness and training, security incident procedures, and contingency plans
- Risk analysis, sanctions policy, workforce clearance procedures, log-in & password management, etc.

Physical safeguards

- Standards: facility access controls, workstation use, workstation security, device & media controls.
- Facility security plans, access control and validation procedures, data backup & storage, etc.

Technical safeguards

- Standards: establish procedures to control access to EPHI, audit activity, protect against tampering, obtain appropriate authentication, & protect EPHI.
- Encryption, decryption, authentication mechanisms.

Expand "Covered Entity" Definition

- Include "any person who knowingly stores or transmits individually identifiable health information in electronic form for any business purpose related to the substance of such information."

Consequences of revised definition

- Many more PHI users will need to obtain authorization from data subjects, including marketers

Excessive discretion

- Security Rule allows covered entities to choose means by which to “reasonably & appropriately” implement standards
- Challenge: create fixed rules for dynamic technical domain

Best Practices Standard

- Requirement: "make reasonable efforts to identify and employ best practices relating to security measures, software development, validation and maintenance, and software system administration that are either commonly used by similarly-situated business entities or governmental institutions or can be clearly demonstrated to be superior to best common practices."

Vendors and products

- Vendors should be certified by government or certifying agencies
- ISO/IEC standards (ISO 27799 Health Informatics)
- CERT
- Turnkey solutions (Advanced MD, HipaaManager HCAT & others)

Enforcement

- As of March 2008 DHHS received 34,771 complaints and investigated 8,923.
- No violation was found in 33% and “corrective action obtained” in 67%
- No civil fines imposed & only 4 criminal actions prosecuted.

Compliance – summer 2006 survey (178 providers, 42 payers)

- Only 56% of providers & 80% of payers have complied
- These have not implemented all required standards
- 39% of providers & 33% of payers suffered security breaches in first half of 2006.

Private Cause of Action

- Private cause of action would enhance deterrence and provide meaningful remedy

Articles

- In Sickness, Health & Cyberspace: Protecting the Security of Electronic Private Health Information
  - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=931069, 48 Boston College Law Review 331 (2007)
- Securing the HIPAA Security Rule
  - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=953670, 8 J. Internet L. 1 (2007)