Implementing the HIPAA Security Rule in the Employer Context

Kate Wakefield, CISSP/MLS/MPA
Information Security Analyst, Costco Wholesale
CISSP-Discuss list moderator
Kate@matrix-magi.com or kwakefield@costco.com
Presentation at HIPAA Summit West – June 6, 2003
Your Presenter

- Those pesky initials (CISSP, MPA, MLS).
- Currently focused on Privacy and Information Security compliance at Costco Wholesale.
- Costco is a Covered Entity for the Pharmacy, as well as in the ‘Employer Context’.
- Member of IAPP, IEEE, ABA, Board member for ISSA Puget Sound Chapter.
- Teach in Information Security BA program at ITT Technical College, sometimes at Bellevue Community College, previously at ESU – KS.
Standard Disclaimers

As they say in Internetish “IANAL” – to obtain legal advice please consult a lawyer who specializes in HIPAA and privacy law.

My opinions are my own -- not my employers’, my family’s or my pets’.

To do HIPAA Security right, you must do a risk assessment of your organization and assess its risk tolerance, technical expertise, and sensitivity of the data you handle daily.
HIPAA  Security regulations

◆ A bit of history ...
  ■ The Draft Security regulations.
  ■ The Preamble to the current regulations.
  ■ So we’re safe until April 2005, right?

◆ Security and Privacy are intimately related. As some have stated, it is impossible to comply with HIPAA Privacy without enacting security controls NOW.
The Employer Context

- The ‘stealth’ group of Covered Entities.
- HIPAA covers employers directly as a group health plan (as defined in ERISA) or a health plan (as defined in HIPAA regs).
- Exemption only for ERISA plans with fewer than 50 participants if they are self-administered.
- Therefore all but the smallest are included.
How to be compliant?

- The Security Rule is final, now what?
- Not simply a matter of installing the right hardware, or designating a security officer.
- The focus is on organization-specific analysis of risks based upon what is ‘reasonable’ and ‘appropriate’ for the size, complexity, and degree of automation utilized.
- Determine vulnerabilities, their probability of occurrence, and utilize risk management to select mitigation strategies.
Standards must be implemented, but some flexibility is given to determine the best organizational fit:

- “specifications may not be applicable to all entities based on their size and degree of automation.”
- Organizations must conduct an assessment of each specification to determine whether it is reasonable and appropriate to its “environment when analyzed with reference to the likely contribution to protecting the entity’s protected health information”
- If choosing not to implement, must document why it wouldn’t be reasonable and appropriate for the specific instance, and
- Still implement an equivalent alternative measure to meet the standard. (Emphasis Mine.)
Security Rule Structure

- The rule is comprised of ‘Standards’ in three categories: Administrative, Physical, and Technical.
- The standards may be further divided into implementation specifications which are labeled ‘Required’ or ‘Addressable’.
- All standards must be implemented with reasonable and appropriate safeguards.
Overarching Goals *

Covered entities must:

- Ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.
- Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required under the privacy rules.
- Ensure compliance by its workforce.

* According to Bill Braithwaite (see Bindview reference)
Security Regs Nutshell
Overview

- 9 Administrative Safeguard Standards
  - 12 Required Implementation Specifications
  - 11 Addressable Implementation Specifications
- 4 Physical Safeguard Standards
  - 4 Required Implementation Specifications
  - 6 Addressable Implementation Specifications
- 5 Technical Safeguard Standards
  - 4 Required Implementation Specifications
  - 5 Addressable Implementation Specifications
Administrative Safeguards
45 CFR 164.308(a)(1)

Standard: Security Mgmt Process

Risk Analysis (R): “Accurate and thorough assessment of potential risks and vulnerabilities”

Risk Management (R): Security measures “sufficient to reduce risks and vulnerabilities”

Sanction Policy (R): for failure to comply with security policies and procedures.

Information System Activity Review (R): regular review of audit logs, access reports, and security incident tracking reports.
Administrative Safeguards
45 CFR 164.308(a)(2)

Standard: Assign Security Responsibility

- No additional specification. The FAQ site makes it clear that although in an organization of any size, you will need multiple people to implement an effective security program, you MUST identify ONE person who is ultimately accountable for the security program.
Administrative Safeguards
45 CFR 164.308(a)(3)

Standard: Workforce Security

- Authorization and/or supervision (A): combines two previously separate requirements [see preamble p.8348]
- Workforce Clearance Procedures (A): determine whether access is appropriate. May include background checks.
- Termination Procedures (A): to remove access to PHI when employment ends or when an individual’s job changes to no longer require access.
Administrative Safeguards
45 CFR 164.308(a)(4)

Standard: Information Access Management

- Isolate health care functions (R): "Restricting access to those persons and entities with a need for access is a basic tenet of security." [p.8349]
- Access authorization (A): policies and procedures to grant users access to systems with PHI.
- Access establishment and modification (A): policies and procedures to establish, document, review, and modify users’ access authorizations.
Administrative Safeguards
45 CFR 164.308(a)(5)

Standard: Security Awareness & Training
Training required for ALL of the workforce, even temps – not simply a one-time ‘orientation’ either.

- Security Reminders (A)
- Protection from malicious software (A): procedures for updating antivirus software, training on detecting and reporting viruses
- Log-in Monitoring (A): actively monitor failed login attempts and report ‘discrepancies’
- Password Management (A): train users on selection of passwords, proper safeguarding
Administrative Safeguards
45 CFR 164.308(a)(6)

Standard: Security Incident Procedures

- **Response and Reporting (R):** formal incident reporting (internal) and response procedures. Mitigate harmful effects, document security incidents and their outcomes.

- **KW Note:** In larger organizations, this means development of a formalized Computer Incident Response Team, as well as provision of minimum level forensics training to system administrators (when/how to report suspected incidents).

- A security incident is defined as “the attempted or successful unauthorized access, use, disclosure, modification or destruction of information OR interference with system operations in an information system” [45 CFR 164.304 (2003), p.8340]
Administrative Safeguards
45 CFR 164.308(a)(7)

Standard: Contingency Planning
Plan for both natural disasters and system failures.
- Data Backup Plan (R)
- Disaster Recovery Plan (R)
- Emergency Mode Operation Plan (R)
- Plan testing and revision procedures (A)
- Applications & data criticality analysis (A)

[Note: Sounds like the CISSP or CISA domain materials, for those who know of the certs.]
Administrative Safeguards
45 CFR 164.308(a)(8)

Standard: Evaluation

“Perform a periodic technical and non-technical evaluation...” The extent to which the policies and procedures implemented meet the rule should also be evaluated (according to PWC).

Removed from Final Standard:

“Certification lingo” (the term is overloaded), Configuration Management and Formal Mechanism for Processing records.
Physical Safeguards
45 CFR 164.310(a)(1)

Standard: Facility Access Controls

Policies and procedures to limit physical access to information systems, while permitting authorized access.

- Contingency operations (A): ensure that access is available in disaster recovery / emergency.
- Facility security plan (A): safeguard facility and equipment against unauthorized access, tampering, and theft
- Access Control and Validation Procedures (A): access to facilities based on role, including visitor control
- Maintenance Records (A): document repairs and modifications to any physical components of security (for example, hardware, walls, doors, and locks)
Physical Safeguards
45 CFR 164.310(b)

Standard: Workstation Use
No separate specification - policies and procedures to specify proper workstation functions (e.g. an acceptable use policy). However: see preamble and draft regs.

Standard: Workstation Security 164.310(c)
No separate specification - physical safeguards to restrict access to authorized users.
NOTE: draft rule specified locking workstations and session logoffs. More flexibility in final rule.
Physical Safeguards
45 CFR 164.310(d)(1)

Standard: Device and media controls

Electronic media is defined in 160.103 to include all type of storage media (hard drives, optical, tape, diskettes)

- Disposal (R): policies and procedures to address final disposition of storage media and devices.
- Media Re-Use Policy (R): procedures to remove PHI from PCs & media before re-using them (even internally).
- Media Accountability (A): maintain records of the movement of hardware and electronic media.
- Data backup & storage (A): “Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.”
Technical Safeguards
45 CFR 164.312(a)

Standard: Access control

“Implement technical policies and procedures ... to allow access only to those persons or software programs that have been granted access in [164.308(a)(4)]”

- Unique userid (R): assign a unique name and/or number for identifying and tracking user identity.
- Emergency access procedure (R): establish procedures for obtaining necessary electronic PHI during an emergency.
- Automatic logoff (A): Implement electronic procedures to terminate an electronic session [or application] after a predetermined period of inactivity.
- Encryption & Decryption (A): use of file encryption for access control to ‘data at rest’.
Technical Safeguards
45 CFR 164.312(b)

Standard: Audit controls 164.312(b)
No separate specification - “implement hardware, software or procedural mechanisms that record and examine” system activity.

NOTE: I.S. Audit is a well-understood field, compared to information systems security. See http://www.isaca.org - CISA, CISM
Technical Safeguards
45 CFR 164.312(c)(1)

Standard: Integrity 164.312(c)(1)
Defined as protection against improper alteration or destruction.

Electronic mechanisms (A): preamble gives the examples of error-correcting memory and magnetic disk storage as well as use of digital signatures and check sums.
Technical Safeguards
45 CFR 164.312(d)

- Standard: Person or Entity Authentication
  164.312(d)
  No separate specification.

Again, Information Security glossaries have well-defined terms for Identification, Authentication, and Authorization.
Technical Safeguards
45 CFR 164.312(e)(1)

Standard: Transmission security

- **Integrity Controls (A):** ensure that electronically transmitted PHI is not improperly modified in transit without detection.

- **Encryption (A):** use it “whenever appropriate”.

  **NOTE, imho:** Any routine transactions of PHI sent over the Internet must be encrypted! Evaluate probability of interception, and risk.

  Email encryption is an understandably big problem. However, solutions are becoming interoperable and will be solidified as your partners make their choices.
Organizational Requirements
45 CFR 164.314

Standard: Business associate contracts (R) or other arrangements.
- Lots of legalese, see OCR topic at their Frequently Asked Questions site:
  
  http://www.hhs.gov/ocr/hipaa/privacy.html

Standard: Requirements for group health plans 164.314(b)(1).
Standard: Policies and Procedures

Maintain WRITTEN policies and procedures to comply with this subpart, and documentation of any required ‘action, activity, or assessment’.

Remember those addressable specifications? Document your organizational risk analysis and why addressable specifications were (or were not) implemented as specified.
Standard: Required Documentation - specifications

Time Limit (R) - Retain for 6 years from date of creation or the date last in effect, whichever is later.

Availability (R) - Make documentation available to those responsible for implementing the documented procedures.

Updates (R) - Review documentation periodically AND “in response to environmental or operational changes affecting the security of the electronic protected health information.”
Web Resources

- HIPAA Security ‘Hyper-rule’

- Full CFR text for HIPAA regulations:
  - http://aspe.os.dhhs.gov/admnsimp/

- Watch for OCR guidance and FAQs:

- “HIPAA Privacy … Employer Context”
  Epstein Becker & Green, PC  IAPP talk:
Web Resources (continued)

- Davis Wright Tremaine LLP, HIPAA Security Regulations Overview
  - [http://www.dwt.com/practc/hc_ecom/bulletins/02-03_HIPAAASecRules.htm](http://www.dwt.com/practc/hc_ecom/bulletins/02-03_HIPAAASecRules.htm)

- Gigalaw – legal news emailed daily or weekly

- Price Waterhouse Cooper’s HIPAA site
  - [http://www.pwchealth.com/hipaa.html](http://www.pwchealth.com/hipaa.html)

- Bindview HIPAA webinar held March 11, 2003:
  - [http://www.bindview.com/events/GetEvents.cfm?NUM=768](http://www.bindview.com/events/GetEvents.cfm?NUM=768)
  Link is no longer active, but you can request a copy of PDF.
Organizations

- CHITA - Great local cooperative site.
  - http://www.chita.org
- International Assn of Privacy Professionals
  - http://www.privacyassociation.org
- SANS Security rule overview
- SANS is working on a longer publication specifically on HIPAA.
- ABA to publish Corporate Privacy Handbook in fall 2003.
Books

