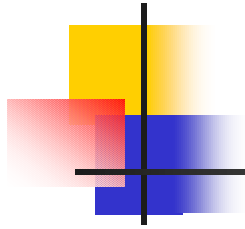




# HIPAA Privacy and Security

---

Kate Wakefield, CISSP/MLS/MPA  
Information Security Analyst  
[Kwakefield@costco.com](mailto:Kwakefield@costco.com)



# Presentation Overview

---

- HIPAA Legislative history & key dates.
- Who is affected? Employers too!
- Privacy Regulation requirements.
- Security Regulation requirements.
- Resources for more information.



# About 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 privacy law.
- My opinions are my own -- not my employers’.
- 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.



# How a law becomes a rule...

---

- Law passed by Congress
- Agency is designated for issuing regulations
  - In the case of HIPAA Privacy, this is the Office of Civil Rights within the Dept of HHS.
- Proposed rule making
- Extensive comment and revision period
- Final rule published in CFR
- 60 days plus two years to compliance date



# HIPAA Key Dates

---

- Security NPRM - 8/12/1998
  - Final Rule not done until 2/20/2003
  - Compliance due by 4/21/2005
- Privacy NPRM – 11/3/1999
  - First 'Final Rule' in CFR on 12/28/2000
  - Guidance issued 7/6/2001
  - Modifications NPRM in CFR on 03/27/2002
  - Final Rule with Modifications 8/14/2002
  - More Guidance issued on 12/03/2002
  - Compliance due by 4/14/2003



# Who is affected?

---

- Health care plans, providers (doctors, dentists), payors, & clearinghouses.
- Self-funded employer health care plans are a covered entity:

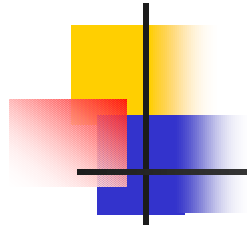
Group health plan as defined in ERISA (unless fewer than 50 employees), plus “any other individual or group plan that provides or pays for health care.



# HIPAA Penalties

---

- Civil penalties:
  - \$100 / violation up to \$25K for each rule.
- Criminal penalties:
  - \$50K / 1 yr prison for a simple violation
  - \$100K / 5 yrs prison for obtaining PHI 'under false pretenses'
  - \$250K / 10 yrs prison for knowingly using or disclosing PHI for commercial advantage, personal gain, or malicious harm.



# Privacy Rule – Org Responses

---

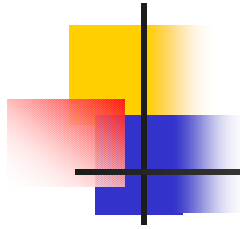
- Appoint a Privacy Officer to be responsible for procedures & training.
- Develop a consumer complaint process.
- Specify sanctions for improper handling.
- Develop training specific to your policy.
- Train all staff who handle PHI on your Privacy policy and related practices.



# Privacy Rule – Practices

---

- Provide notice of privacy practices.
- Obtain authorization for use & disclosure which is not TPO-related.
- Track all disclosures (as consumer may request an accounting of them).
- Retain records for six years.
- Obtain Business Associate agreements from all partner companies.



# How Privacy & Security Relate

---

- Privacy is the right of an individual to control personal information, and not have it disclosed or used without permission.
- Security is the combination of technology, policy, and procedures used to protect the confidentiality, integrity, and availability of information.
- HIPAA specifies physical, technical, and administrative safeguards to ensure privacy.
- Preamble to Security rule spells this out.



# Security Rule Structure

---

- The Security rule is comprised of 'Standards' in three categories (Administrative, Physical, and Technical).
- Standards may be further divided into implementation specifications which are labelled 'Required' or 'Addressable'.
- All standards must be implemented with reasonable and appropriate safeguards.



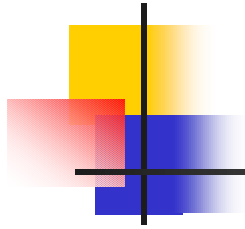
# Overarching Goals \*

---

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)



# How to be compliant?

---

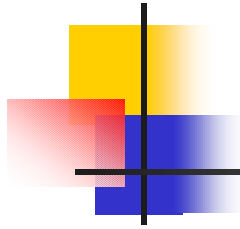
- The Security Rule is final, now what?
- Not simply a matter of installing the right hardware, writing a policy, or designating a security officer.
- Compliance focus is on organization-specific analysis of risks and documentation of decisions.



# 'Addressable' NOT 'Optional'

---

- 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 would not be reasonable and appropriate for the specific instance, and
  - Implement an equivalent alternative measure to meet the standard.



# 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: Assigned Security Responsibility

- No additional specification.
- Identify ONE person who is ultimately accountable for implementation of security.
- NOTE that in larger organizations the security function may require several different people.
- Smaller organizations may combine the Privacy Officer and Security Officer functions.



# 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] regarding hiring and ongoing supervision.
- Workforce Clearance Procedures (A): determine whether access to PHI is appropriate for each position. 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 Mgmt

- 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

Ongoing training required for ALL of the workforce (including temps). Not simply a one-time orientation.

- 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



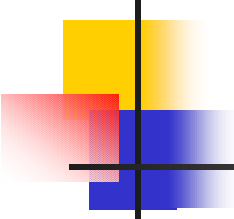
# Administrative Safeguards

## 45 CFR 164.308(a)(6)

---

### Standard: Security Incident Procedures

- Response and Reporting (R): formal incident reporting (internal) and response procedures. Goal is to mitigate harmful effects, document security incidents and their outcomes.
- NOTE: In larger organizations, this means creation of a formalized CIRT (Computer Incident Response Team), as well as training to system administrators on 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)



# Administrative Safeguards

## 45 CFR 164.308(a)(8)

---

Standard: Evaluation

No separate specification - periodic review and “in response to environmental or operational changes” of extent to which policies and procedures meet the Security Rule requirements.

Removed from Final Standard:

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 164.310(b)

No separate specification - policies and procedures to specify proper workstation functions (e.g. an Acceptable Use Policy)

Standard: Workstation Security 164.310(c)

No separate specification - physical safeguards to restrict access to authorized users.

NOTE: draft rule specified automatic locking workstations. 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 (harddrives, 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 reusing 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 user identification (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.



# Technical Safeguards

## 45 CFR 164.312(a) - cont.

---

- 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'.

### Standard: Audit controls 164.312(b)

No separate specification - "implement hardware, software or procedural mechanisms that record and examine" system activity.



# Technical Safeguards

## 45 CFR 164.312

---

### Standard: Integrity 164.312(c)(1)

Protection against improper alteration or destruction of data.

- 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.

### Standard: Person or Entity Authentication 164.312(d)

No separate specification - procedures to verify identity (that each person is who they claim to be). Biometrics and two-factor authentication were originally recommended here.



# 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: PHI sent over Internet should be encrypted!  
Evaluate probability of interception, and risk.  
Email encryption is an understandably big problem.



# Organizational Requirements

## 45 CFR 164.314

---

Standard: Business associate contracts (R) or other arrangements.

- Lots of legalese, see OCR topical Frequently Asked Questions site:

<http://www.hhs.gov/ocr/hipaa/privacy.html>

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



## Policies, Procedures & Documentation 45 CFR 164.316(a)

---

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.



## Policies, Procedures & Documentation 45 CFR 164.316(b)

---

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

---

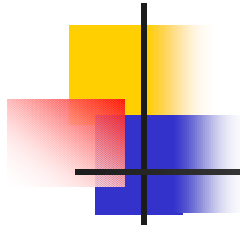
- HIPAA Security 'Hyper-rule'
  - <http://web.interhack.com/publications/hipaasec.php>
- Full CFR text for HIPAA regulations:
  - <http://aspe.os.dhhs.gov/admnsimp/>
- Watch for OCR guidance and FAQs:
  - <http://www.hhs.gov/ocr/hipaa/whatsnew.html>
- HIPAAAction – has good, readable articles
  - <http://www.hipaadvisory.com/action/security/>



## Web Resources (continued)

---

- David Wright Tremaine LLP, Overview
  - [http://www.dwt.com/practc/hc\\_ecom/bulletins/02-03\\_HIPAA\\_SecRules.htm](http://www.dwt.com/practc/hc_ecom/bulletins/02-03_HIPAA_SecRules.htm)
- SANS Security rule overview
  - [http://www.sans.org/rr/policy/HIPAA\\_policy.php](http://www.sans.org/rr/policy/HIPAA_policy.php)
- Gigalaw – legal news, emailed daily or weekly
  - <http://www.gigalaw.com/newsletters/>



# Organizations

---

- Internat'l Assn of Privacy Professionals
  - <http://www.privacyassociation.org>
- Online Discussion Groups:
  - [HIPAA-CISSP@yahoogroups.com](mailto:HIPAA-CISSP@yahoogroups.com)
  - [HIPAAShare@yahoogroups.com](mailto:HIPAAShare@yahoogroups.com)