

HIPAA: The Security Rule What Have We Learned?

**Robyn J. Bartlett, Esq.
Associate General Counsel
Tufts Health Plan**

TUFTS  Health Plan

THE SECURITY RULE:

What's the point?

- **A uniform set of security standards**
- **Evolution of health care industry to electronic transactions**



WHAT TRANSACTIONS ARE COVERED?

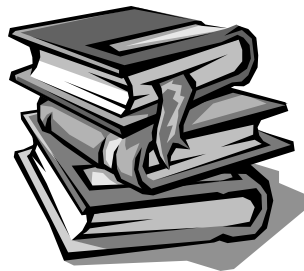
- Security Rule guards e-PHI
- Individually identifiable health information transmitted or maintained in electronic media.
- PHI not in electronic form before its transmission is not covered.

3

TUFTS  Health Plan

GOALS OF THE SECURITY RULE

- Comprehensive and Coordinated
 - Administrative, Physical, and Technical Safeguards
- Scalable
- Technology Neutral



4

TUFTS  Health Plan

GENERAL REQUIREMENTS OF THE SECURITY RULE

- Ensure confidentiality, integrity and availability of the e-PHI
- Protect against reasonably anticipated threats
- Protect against impermissible uses or disclosures
- Ensure compliance by workforce

5

TUFTS  Health Plan

COMPLIANCE DATE

- April 20, 2005 (except for small health plans)
- So.... Why are we still talking about this?



6

TUFTS  Health Plan

HIGH RATES OF NON-COMPLIANCE

- **As of Summer, 2006:***

Payers – 80% compliant

Providers – 56% compliant

* U.S. Healthcare Industry HIPAA survey results, Summer 2006, HIMMS, Healthcare Information and Management Systems Society/Phoenix Health Systems, Copyright 2006 Phoenix Health Systems, Inc.

7

TUFTS  Health Plan

AFTER THE FANFARE ENDS ...THE SECURITY RULE DOESN'T END.....

- **The Security Rule requires ongoing security management. The obligations continue even after the fanfare ends!**
- **Technology changes and improves. Managing security is an iterative process.**



8

TUFTS  Health Plan

STANDARDS AND IMPLEMENTATION SPECIFICATIONS

- Standards and (*in some cases*) Implementation Specifications
- Implementation Specifications are instructions for implementing the corresponding Standard.



9

TUFTS  Health Plan

REQUIRED v. ADDRESSABLE

- “**Required**” Implementation Specifications are mandatory.
- “**Addressable**” Implementation Specifications provide *some flexibility* to covered entity in meeting the applicable Standard.

10

TUFTS  Health Plan

ADDRESSABLE SPECIFICATIONS

- **Assess whether Implementation Specification is “reasonable and appropriate” in covered entity’s environment**
 - If so, implement.
 - If not, document why not and identify and implement equivalent alternative measure if reasonable and appropriate to do so.

11

TUFTS  Health Plan

ADDRESSABLE SPECIFICATIONS

Whether an implemented measure is effective is likely to be determined after the fact.

Think about the Monday Morning Quarterback!



12

TUFTS  Health Plan

ADMINISTRATIVE SAFEGUARDS **OVERVIEW**

1. Security Management Process
2. Assigned Security Responsibility
3. Workforce Security
4. Information Access Management
5. Security Awareness and Training
6. Security Incident Procedures
7. Contingency Plan
8. Evaluation
9. Business Associate Contracts and Other Arrangements

13

TUFTS  Health Plan

KEY ADMINISTRATIVE SAFEGUARDS

- ***STANDARD: Security Management Process – Implement policies and procedures to prevent, detect, contain and correct security violations***
 - ***REQUIRED: Risk analysis***
 - Conduct an accurate and thorough assessment of potential risks to e-PHI – identify all assets with PHI.
 - Huge amount of work!
 - Look at threats to the system – internal and external
 - Vulnerabilities of the system
 - Impact to the organization
 - GAP analysis

14

TUFTS  Health Plan

KEY ADMINISTRATIVE SAFEGUARDS

- **STANDARD: Security Management Process** (con't)

- **REQUIRED: Risk management**
 - Implement security measures to reduce risks – create a Security Infrastructure!
 - Detect and respond to Security “incidents”
 - Intrusions become more sophisticated; technology becomes more sophisticated.
 - Need to keep a pulse on the world of security.



15

TUFTS  Health Plan

KEY ADMINISTRATIVE SAFEGUARDS

- **STANDARD: Security Management Process** (con't)

- **REQUIRED: Sanction policy**
 - Covered Entity has flexibility to determine type and severity of sanctions based upon its security policy
 - HHS guidance: suggests employees sign a statement of adherence to Covered Entity's security policies
- *Are you enforcing your security policies today?*

16

TUFTS  Health Plan

KEY ADMINISTRATIVE SAFEGUARDS

- ***STANDARD: Assigned Security Responsibility***
 - Security Officer (“SO”) to manage and supervise security measures
 - Does the SO have enough help?
 - Does the SO have the right skill sets?
 - Does the SO have “clout” to influence expenditures?

17

TUFTS  Health Plan

KEY ADMINISTRATIVE SAFEGUARDS

- ***STANDARD: Workforce Security – Policies and procedures to ensure that members of workforce have appropriate access to e-PHI***
- “Only people who need to have access, have access.”

18

TUFTS  Health Plan

KEY ADMINISTRATIVE SAFEGUARDS

- **STANDARD: Security Awareness Training – provide reasonable and appropriate training to workforce**
 - **ADDRESSABLE:** Security reminders
 - **ADDRESSABLE:** Protections from malicious software
 - **ADDRESSABLE:** Log-in monitoring
 - **ADDRESSABLE:** Password management (creating/changing/safeguarding)



KEY ADMINISTRATIVE SAFEGUARDS

- **STANDARD: Security Incident Procedures – handling any attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations**
 - **REQUIRED:** Identify, respond to and mitigate harmful effects of and document each security incident and outcome

KEY ADMINISTRATIVE SAFEGUARDS

- **STANDARD: Contingency Plan** – protecting the availability, integrity and security of data during unexpected events or crises

- **REQUIRED:** Data backup plan
- **REQUIRED:** Disaster recovery plan
- **REQUIRED:** Emergency mode operation



These Plans need to be tested and evaluated on an ongoing basis.

21

TUFTS  Health Plan

KEY ADMINISTRATIVE SAFEGUARDS

- **STANDARD: Evaluation** – Periodic evaluation of technical and non-technical security measures in response to changing environment, technology or operations

- “Cannot sit on your laurels”

Are security measures up to par with current operations and current technology?



22

TUFTS  Health Plan

KEY ADMINISTRATIVE SAFEGUARDS

- **STANDARD:** *Business Associate may create, receive, maintain or transmit e-PHI for CE if “satisfactory assurances”*
 - **REQUIRED:** Written contract that requires Business Associate to:
 - Implement administrative, physical and technical safeguards
 - Ensure that subcontractors also comply
 - Report security incidents
 - Authorize termination if Business Associate violates contract

These requirements should be in a standard template.

23

TUFTS  Health Plan

PHYSICAL SAFEGUARDS OVERVIEW

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

24

TUFTS  Health Plan

KEY PHYSICAL SAFEGUARDS

- **STANDARD: Facility Access Controls – policies to limit physical access to systems and facilities where e-PHI is housed**
 - Always ask: *Where do you house e-PHI? Is it safe from unauthorized access?*
 - Covered Entity needs to keep track of repairs to locks, video cameras, and access systems (like badge readers).

25

TUFTS  Health Plan

KEY PHYSICAL SAFEGUARDS

- **STANDARD: Workstation Security – implement physical safeguards that prevent unauthorized access to workstations (Also need policies).**



Examples: Locating workstations in secured areas, privacy screens, screen savers.

26

TUFTS  Health Plan

KEY PHYSICAL SAFEGUARDS

- ***STANDARD: Device and Media Controls***
– policies that govern the receipt and removal of hardware and media that contain e-PHI
 - ***REQUIRED:*** Disposal of hardware and electronic media to ensure PHI is removed/destroyed
 - ***REQUIRED:*** Remove e-PHI from electronic media before making available for reuse

27

TUFTS  Health Plan

TECHNICAL SAFEGUARDS OVERVIEW

1. Access Controls
2. Audit Controls
3. Integrity
4. Person or Entity Authentication
5. Transmission Security

28

TUFTS  Health Plan

KEY TECHNICAL SAFEGUARDS

- **STANDARD: Access Control – policies to prevent unauthorized access**
 - **REQUIRED:** Unique user identification
 - Passwords (unique and strong); PIN numbers; biometrics
 - **REQUIRED:** Emergency access procedures
 - **ADDRESSABLE:** Automatic logoff
 - **ADDRESSABLE:** Encryption and decryption
 - Can be a good solution for laptop users.



29

TUFTS  Health Plan

KEY TECHNICAL SAFEGUARDS

- **STANDARD: Audit Controls – implement mechanisms that record and examine activity with regard to e-PHI**

Audit Trail = a record showing who accessed the computer system and what operations the system performed.



- ***Need to have audit trails and need to have someone review them!***

30

TUFTS  Health Plan

KEY TECHNICAL SAFEGUARDS

- **STANDARD: Transmission Security** – *technical security measures to guard against unauthorized access while e-PHI is being transmitted over an electronic communications network*
 - **ADDRESSABLE:** Integrity controls
 - **ADDRESSABLE:** Encryption
 - **HHS guidance:** Covered Entities should prohibit transmission of e-PHI over an open network (e.g. the Internet).

31

TUFTS  Health Plan

POLICIES, PROCEDURES AND DOCUMENTATION

- **STANDARD: Implement reasonable and appropriate policies and procedures** to comply with the Security Rule.
- **STANDARD: Documentation** – *maintain a written record of the policies and procedures implemented, and of any action, activity or assessment required by the Security Rule*
 - **REQUIRED:** Time limit – 6 years
 - **REQUIRED:** Availability – to those responsible for implementation
 - **REQUIRED:** Updates

32

TUFTS  Health Plan

Internal vs. External Resources

Selecting the Security Consultant

- Experience
- No conflicts
- References
- Financial stability
- Request for Proposal/Information
- Use of subcontractors



33

TUFTS  Health Plan

Contracting with the Security Consultant

Create a contract you can live with:

Scope of Services

- Refer to Security Rule provisions
- Specify methodology for risk assessment
- Description of deliverables
- Commencement and completion dates

Fees

- Payment terms
- Milestone based vs. date-certain
- Not to exceed hourly rates
- Audit rights



34

TUFTS  Health Plan

Other Important Contract Provisions

Indemnification

- Indemnity for IP claims, breach of confidentiality, property damage, personal injury or death
- Insurance representations!

Ownership

- Make sure ownership is in customer from time of creation or that customer has unrestricted license rights to use work product for internal business purposes

35

TUFTS  Health Plan

Important Contract Provisions

Warranties

- *Dream Warranty*: Covered Entity will achieve HIPAA compliance
- Service warranty in accordance with professional standards
- Intellectual property and all necessary rights

Termination

- Convenience
- Breach after cure period
- Bankruptcy; insolvency



Confidentiality

- HIPAA
- Confidentiality Language

36

TUFTS  Health Plan

Acquisition of Technology post-HIPAA

- ◆ **HIPAA Business Associate Agreement**
 - Makes representations about compliance with Security Rule

- ◆ **Going the Extra Mile Assessing Vendors**
 - Internal Resources
 - Penetration Testing
 - Contractual Requirements Based on Findings

37

TUFTS  Health Plan

Acquisition of Technology post-HIPAA

Outsourcing

- Increases risk of data security breaches
- Obtain indemnities
- Ensure that subcontractors are fully insured against any data breaches.
 - Review Certificates of Coverage!



38

TUFTS  Health Plan

In the News...Enforcement Issues

2005 – The Kaiser Permanente Fine

- ◆ Kaiser Permanente division fined \$200K for data breach by CA Department of Managed Health Care
- ◆ Kaiser created systems diagram Web site used as testing portal for IT staff. Site contained confidential patient information: names, addresses, telephone numbers, lab results.
- ◆ Web site languished in accessible format for up to four years.

39

TUFTS  Health Plan

In the News...Enforcement Issues

2006 – The Year of the Stolen Laptop

- ◆ Many health plans, hospitals, government health agencies reported stolen laptops.
- ◆ Also, large number of PC thefts
- ◆ Lessons learned
 - Remote access is a critical security issue
 - Physical security is as important as technical security
 - Encryption = solution worth considering
 - *What are you storing on your hard drive?*

40

TUFTS  Health Plan

In the News...Enforcement Issues

Recent HHS Guidance (January 2007)

on remote use, laptops, PDA's offsite access to e-PHI



Covered Entity should be “*extremely cautious*” about allowing offsite use or access to e-PHI.

41

TUFTS  Health Plan

In the News...Enforcement Issues

HHS Risk Management Strategies for Remote Usage

- ◆ 2-Factor Authentication for remote access
- ◆ Establish “time-outs” for session termination
- ◆ Use/update virus protection software
- ◆ Prohibit downloading of e-PHI to remote systems without operational justification
- ◆ Prohibit transmission of e-PHI over an open network (i.e. the Internet)

42

TUFTS  Health Plan

In the News...Enforcement Issues

- ◆ Although government receives many complaints under HIPAA, *not yet imposed a single civil fine.*
- ◆ 2 criminal cases under Privacy Rule, but nothing under the Security Rule...

– How do you convince your company of the importance of compliance?

43

TUFTS  Health Plan

In the News...Enforcement Issues

Liability for HIPAA Violations

Civil Liability

- Under HIPAA, DHHS may impose fines of \$100 per violation up to \$25,000 per person per year for negligent violation of a single standard

Criminal Liability

- DHHS may make a criminal referral to Department of Justice for a HIPAA violation with fines up to \$250,000 and one to ten years imprisonment

44

TUFTS  Health Plan

In the News...Enforcement Issues

- ◆ Individuals care intensely about security of medical information.
- ◆ On average, U.S. healthcare organizations spend 1.1% less on security and privacy in IT budgets than other industries. *
- ◆ Largest risk is bad publicity that can follow a breach.

*Source: PricewaterhouseCoopers/CIO Global State of Information Security

45

TUFTS  Health Plan

HYPOTHETICAL

- ◆ Jane is an employee in the HR department of Big Hospital. She is expecting her first child.
- ◆ Bob is an employee in the IS department of Big Hospital. At the water cooler, Bob tells Bill, also an employee in the IS Department and friend of Jane's, that Jane is going to have a boy, and that the child has significant medical problems.
- ◆ Jane finds out and files a complaint with Big Hospital's senior management. Senior management calls the Security Officer and asks that she immediately address the problem.

46

TUFTS  Health Plan