

MARTI ARVIN

University of Louisville
Privacy Officer

Phone: 502-852-3803
Fax: 502-852-3855
Email: marti.arvin@louisville.edu

HIPAA Security

Will your practice be ready?
Practical Tips to Help You Prepare

AGENDA

- Intent of the Security Rule
- Components of the Security Rule
- Things to begin thinking about
- Q & A

3

Security versus Privacy

- Privacy rule identifies what is to be protected and outlines the individual's rights to control access to their PHI
- The security rule defines how to protect PHI in electronic form
 - The security rule only applies to PHI maintained or transmitted in electronic form, called ePHI
- You can have security without privacy but you cannot have privacy without security

4

Intent of the Security Rule

- Security rule is intended to be technology neutral
- The rule is intended to be scalable
- The security rule is intended to protect the confidentiality, integrity and availability of ePHI
 - Confidentiality – ensuring that only those individuals who are supposed to access ePHI do
 - Integrity – ensuring that the ePHI input today is the ePHI that is retrieved tomorrow, next week, next year, etc.
 - Availability – ensuring that ePHI is available to those who need it when they need it

5

Intent of the Security Rule (cont.)

- The security rule is also intended to protect ePHI against any reasonably anticipated threats or hazards, and improper use or disclosure



6

Components of the Security Rule

- Three types of safeguards
 - Administrative
 - Physical
 - Technical
- DOCUMENTATION, DOCUMENTATION, DOCUMENTATION
- Policies and Procedures

7

Three Safeguards

- The three safeguards of administrative, physical and technical are broken down into standards
 - 18 standards total
- The standards have corresponding implementation specifications
 - 36
- The implementation specifications are either required or addressable
 - 14 required and 22 addressable

8

Security Rule Implementation Specifications

- Required – this means that you do not have a choice, you must implement the specification
 - Example: A risk analysis to identify the risks and vulnerabilities to the ePHI maintained by the covered entity must be done in order to eliminate or minimize those risks.
 - If you don't know your systems strengths and weaknesses you cannot properly evaluate whether changes need to be made.

9

Security Rule Implementation Specifications

- Addressable – this means a covered entity must analyze the specification to determine if it is reasonable and appropriate in the environment of that covered entity.
- If it is reasonable and appropriate the covered entity must implement the specification.
- If it is not considered reasonable and appropriate the covered entity must do one of the following:
 - Implement another equivalent measure or
 - Not implement the specification or an equivalent measure, if the standard can otherwise be met.

10

Documentation and P & Ps

- You must document your processes and decision making – the security rule requires it
- For all of the implementation standards and specifications you must have a corresponding policy and procedure unless you do not implement the specification

11

Administrative Safeguards

- Security Management Process
- Assign Security Responsibility
- Workforce Security
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts & Other Arrangements

12

Security Management Process

- Risk Analysis (R)
 - Evaluate the risks to the CIA of the ePHI held by your practice
- Risk Management (R)
 - Implement measures to reduce risk to a reasonable and appropriate level
- Sanctions Policy (R)
- Information systems activity review (R)
 - Review of audit logs, access reports, and security incident tracking reports.

Risk of occurrence	Liability if occurs		
	HIGH	MEDIUM	LOW
HIGH	1	1	2
MEDIUM	1	2	3
LOW	2	3	3

Ways to Handle Risk

- Mitigation
 - Take measures to reduce or eliminate the risk
- Acceptance
 - Do nothing about the risk based on a conscious decision that you accept the consequences if the threat or hazard occurs
- Transfer
 - Buy insurance against the risk
 - Outsource the function to someone better capable of reducing the risk

Assign Security Responsibility (R)

- Final responsibility for security must be assigned to one individual to
 - Manage and supervise
 - The use of security measures to protect data, and
 - The conduct of personnel in relation to the protection of data
- The security official will have the “overall final responsibility for the security of the entity’s electronic protected health information”

68 Federal Register, No. 34, 8347

16

Workforce Security

- Authorization and/or Supervision (A)
 - Oversight of employee access to ePHI.
 - Is the level of access appropriate for the employee’s job function?
- Workforce Clearance Procedures Termination Procedures (A)
 - Reference checks
 - Background checks
 - Termination of access w/termination of individual

17


Information Access Management

- Isolating Healthcare Clearinghouse Function (R)
 - Do you bill for another physician practice or health care provider?
 - Not someone who is part of your practice
 - Even if you don’t have a clearinghouse function you must document that this implementation specification does not apply
- Access Authorization (A)
 - Who can access what?
- Access Establishment & Modification (A)
 - How does one get access?
 - How is one’s access changed when their job function changes?
 - If you are small practice then individuals may have access to everything and modification would not be necessary

18

Security Awareness & Training (A)

- A covered entity should train the workforce as reasonable and appropriate to carry out their functions in the facility
- Security Reminders (A)
- Protection from malicious software (A)
 - You should control what is loaded on the practices' computer
 - Maintain updated virus protection software
- Log-in Monitoring (A)
 - Limit and Monitor log-in attempts
- Password Management (A)
 - Change passwords at appropriate intervals
 - Need to change password is inversely related to the strength of the password



19

Security Incident Procedures (R)

- Response and Reporting
 - You must have P & Ps to address security incidents
 - Definition "the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with systems operations in an information system containing PHI".
 - This is not only "hackers", it may include
 - Misuse of a logon and password
 - Attempt to physically access a computer room
 - Theft of a computer
 - Misplacement of a computer disk containing ePHI
 - You probably want to define this in broader terms that simplify ePHI but you are not required to under the Security Rule

20

Contingency Plan

- Data Back-up Plan (R)
 - A retrievable exact copy stored in a secure separate location
- Disaster Recovery Plan (R)
 - Procedure to restore lost data
- Emergency Mode Operation (R)
 - How is data secured?
 - What data do you need in order of priority?
 - Level of detail will depend on size & quantity of ePHI
- Testing & Revision Procedure (A)
 - Occasionally test & as appropriate revise contingency plan
- Application and Data Criticality Analysis (A)
 - Prioritize your systems

21

Evaluation (R)

- Ongoing periodic analysis of your systems to ensure continued compliance with the standards of the Security Rule based on changing operations or environment

22

Business Associate Contracts (R)

- Under the privacy rule BAs are required to assure that certain others also protect the privacy of PHI.
- Under the security rule BAs will be required to agree, in a written contract, to ensure the security of ePHI the BA receives.

23

Business Associate Contracts (cont.)

- What does this mean to you?
 - If you have a business associate contract with an external party you must include language to address the security rule requirements.
 - The language is very similar to what is required for a BA agreement under the privacy rule.
 - One distinct difference is the requirement that the BA report to the CE **ANY** security incident of which it becomes aware.
 - You probably want to clarify the definition of a security incident in the BA.

24

Physical Safeguards

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device & Media Controls

25

Facility Access Controls

- Contingency Operations (A)
 - Plan for access when you have to implement your contingency or emergency operation plan
- Facility Security Plan (A)
 - How does one access your facility?
 - Do different areas require different access?
 - How is PHI secured within your facility?
 - Both ePHI and PHI
- Access Controls & Validation Procedures (A)
- Maintenance Records (A)

26

Workstations

- Workstation Use (R)
- Workstation Security (R)

27

Device & Media Controls

- Disposal (R)
- Media Re-use (R)
- Accountability (A)
- Data Back-up & Storage (A)

28

Device and Media Controls (R)

- Applies to hardware and portable media and devices
 - Whose device is it?
 - What level of security is on the device?
- A documented policy and procedure must be in place to address disposal and re-use
 - Donation of equipment
 - Re-use of CDs, disks and DVDs

29

Access Controls (R)

- Unique User ID is required
- An emergency access procedure is required
- Automatic Logoff is addressable
- Encryption and Decryption are addressable

30

Technical Safeguards

- Access Controls
- Audit Controls
- Integrity
- Person & Entity Authentication
- Transmission Security

31

Access Controls

- Unique User Identifier (R)
- Emergency Access Procedure (R)
- Automatic Logoff (A)
- Encryption & Decryption (A)

32

Audit Controls (R)

- A covered entity must be able to record and examine system activity.
- What you want to be able to record and examine is based on your own risk analysis.

33

Other Standards

- Integrity (R)
 - Mechanism to Authenticate ePHI
- Person or Entity Authentication (R)
 - Create a mechanism to ensure that the person or entity seeking access to ePHI is really who they say they are such as user names and passwords.

Transmission Security

- Integrity Controls (A)
 - Methods to ensure that data is not tampered with while in transition
 - Who can change data?
- Encryption (A)
 - Consider methods to secure ePHI both in transition and at rest, particularly in certain devices such as PDA, laptops, CDs, zips, etc.

Things to think about

- Business Associate Contracts
- Training
- Appointment of a Security Officer
- Audit controls
- Access controls
- Device and media controls



QUESTIONS



37
