NAVIGATING THROUGH THE HIPAA SECURITY RULE

FRIDAY, APRIL 22, 2022

1

Holly Schlenvogt

Privacy & Security Consultant / Owner
HRT Consulting, LLC
(262) 468-4291 (Office)
hschlenv@hrt-consulting.com

http://hrt-consulting.com

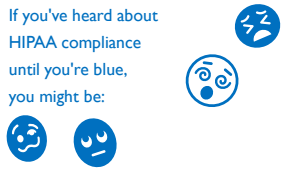
2

Today's Discussions
Navigating through the HIPAA Security Rule

- Recap of HIPAA Security Rule requirements
- Explore key requirements:
  - Administrative, physical, and technical controls
  - Policies and procedures (topics of discussion)
  - Completing security risk analyses and managing identified risks
  - Training

3

If you've heard about HIPAA compliance until you're blue, you might be:



HIPAA–thermic!

4

HIPAA Security Rule Recap: Seven Key Sections

1. General Rules (164.306)
2. Administrative Safeguards (164.308)
3. Technical Safeguards (164.310)
4. Physical Safeguards (164.312)
5. Organizational Requirements (164.314)
6. Policies and Procedures and Documentation Requirements (164.316)
7. Compliance Dates for the initial implementation (164.318)

5

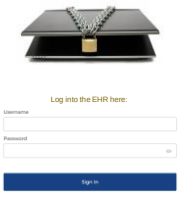
Key Security Rule Definitions

- **Electronic protected health information** (**ePHI**) means individually identifiable health information:
  - Transmitted by or maintained in electronic media;
  - That is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:
    - Past, present or future physical or mental health or condition of an individual
    - The provision of health care to an individual
    - The past, present, or future payment for the provision of health care to an individual

6

Key Security Rule Definitions

- **Confidentiality**: ePHI is not available or disclosed to unauthorized persons.
- **Integrity**: ePHI is not altered or destroyed in an unauthorized manner.
- **Availability**: ePHI is accessible and usable on demand by an authorized person.



7

Flexibility of the HIPAA Security Rule

- Allows organizations to chose the ways they protect ePHI. When making security measure decisions, consider:
  - Size, complexity, & capabilities
  - Technical, hardware, and software infrastructure
  - Costs
  - Likelihood and possible impact of potential risks to ePHI

8

Small Organizations

- Your "environment" may look like this:
  - Small budget
  - Lack of space
  - Limited or no in-house technical expertise
  - Privacy/Security Officer is the Office Manger who also fills in for almost all roles

= Security compliance remains on the back burner

- How have you overcome this?

9

Implementation Specifications: Required vs. Addressable

- **Required**: it is required

- **Addressable**:
  it "…*is not optional; rather, if an organization determines that the implementation specification is not reasonable and appropriate, the organization must document why it is not reasonable and appropriate and adopt an equivalent measure if it is reasonable and appropriate to do so*"

10

Source: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es

10

Topics of Discussion: Examples of "Joint" Privacy and Security Policies and Procedures (P&Ps) to Write ***and*** Implement

- Privacy and security oversight
- Privacy and security incidents
  - Breach notifications
- Business associate
- Facility access
- Disposal
- Group health plan
- Information retention

11

11

Topics of Discussion: Examples of Security P&Ps to Write ***and*** Implement

Confidentiality, Integrity, and Availability of ePHI

- Risk analysis and risk management
- Contingency plan
- Data backup and media management
- Malicious software protections
- Auditing
- Facility maintenance
- System access
  - Remote access
- Technical access control
- System build / change control
- Service providers
- New organization acquisition
- Information Retention

12

12

1. HIPAA Oversight Policy

- Write ***and*** implement P&Ps:
  - A. General Oversight
  - B. Retention
  - C. Training

Assign a Security Officer

13

13

2. Risk Analysis and Risk Management Policy

- Write ***and*** implement Risk Management policies and procedures (P&Ps)
- Complete a risk analysis to identify threats and vulnerabilities
  - Rank threats and vulnerabilities
  - Address risks
- Complete assessments on an ongoing basis

14

14

3. Contingency Plan Policy

- Write ***and*** implement P&Ps to:
  - Respond to different types of emergencies and continue critical business
  - Restore access to ePHI
  - Assess the criticality of applications and data
  - Allow appropriate access to facilities during emergencies
  - Describe how users will access ePHI during emergencies
  - Test and revise contingency plans

15

15

4. Data Backup and Media Management Policy

- Write ***and*** implement P&Ps to:
  - Backup ePHI
  - Secure ePHI when transported
  - Maintain logs of devices when moved (that have ePHI on them)
  - Move electronic media

16

16

5. Malicious Software Protections Policy

- Write and implement P&Ps to:
  - Guard against, detect, report, and remove malicious software through the use of anti-malware software (e.g., viruses, Trojan horses, and worms)
  - Have a timely patch management program
  - Have properly configured firewalls
  - Monitoring of the above

17

17

6. Auditing Policy

- Write ***and*** implement P&Ps for:
  A. Log-in Monitoring
  B. User Auditing

18

18

7. Incidents Policy

- Write ***and*** implement P&Ps for:
  - A. Security Incident Response (SIR)
  - B. Sanctions
  - C. Breach Notifications

19

19

8. System Access Policy

- Write ***and*** implement P&Ps to protect ePHI and restrict access:
  - A. Roles – provide minimum necessary access
  - B. Authorize, modify, and terminate access
  - C. Auto Log-off
  - D. Health Care Clearinghouse
  - E. User authentication and passwords
  - F. Workstation use & safeguards
  - G. Social Media
  - H. Personal accounts
  - I. Personal devices

20

20

8.5. Remote Access Policy

- Write ***and*** implement P&Ps to:
  - Authorize remote access
  - Outline required administrative, physical, and technical controls
  - Define remote user responsibilities

21

21

9. Business Associate (BA) Policy

- Write ***and*** implement P&Ps to:
  - Obtain Business Associate Agreements (BAAs)
  - Maintain copies of BAAs
  - Have an incident reporting process for BAs
  - Monitor BAs

22

22

10. Facility Access Policy

- Write ***and*** implement P&Ps to:
  - Limit physical access to areas that house ePHI to only those that need access to it
  - Safeguard the facilities and ePHI systems

23

23

11. Facility Maintenance Policy

- Write ***and*** implement P&Ps to:
  - Document repairs and changes made to buildings

24

24

12. Disposal Policy

- Write ***and*** implement P&Ps to:
  - Destroy ePHI on hardware, devices, etc..
  - Consider including disposal of hard copy PHI in this policy as well
  - Remove ePHI from electronic media before being used by anyone else

25

25

13. Technical Access Control Policy

- Write ***and*** implement P&Ps for:
  - A. Encryption
    - At rest
    - In transit
  - B. System Isolation
  - C. Integrity
    - Prevent ePHI from being improperly changed or destroyed
    - Put in place ways to verify ePHI was not altered or destroyed in an unauthorized manner

26

26

Encryption & Preventing a "Breach of Unsecured PHI"

Safe harbor

- **Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals:**
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html
  - Examples (see above website for more):
    - Data at rest: NIST SP 800-111
    - Data in motion: NIST SP 800-52, NIST SP 800-77, FIPS 140-2 validated
- How do you know it meets one of the above?
- http://www.eetimes.com/document.asp?doc_id=1279619

27

27

14. Group Health Plan Policy

- Write ***and*** implement P&Ps
- If the Covered Entity sponsors a self-insured health plan:
  - Include in the plan documents that they reasonably & appropriately safeguard ePHI that they create, receive, maintain, or transmit on behalf of the group health plan
- Include that they report security incidents to the group health plan

28

28

15. System Build / Change Control Policy

- Write ***and*** implement P&Ps that outline steps to take when making changes to the IT infrastructure
  - Document and obtain approvals for change plans
  - Test changes made before "going live" with them
  - Document and follow baseline standards

29

29

16. Service Providers Policy

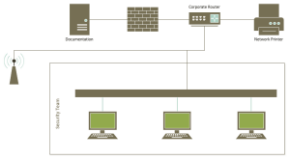
- Write ***and*** implement P&Ps that define expectations for acquiring and managing service provider relationships

30

30

17. New Organization Acquisition Policy

- Write ***and*** implement P&Ps that outline how to secure ePHI while integrating an acquired organizations into your environment



31

31

18. Information Retention Policy

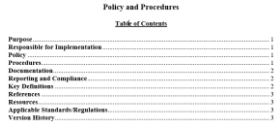
- Write ***and*** implement P&Ps to securely retain all ePHI and security related activities for required timeframes

32

32

Write ***and*** Implement P&Ps

- Your P&Ps will include numerous administrative, physical, and technical controls
  - Fully implement them throughout the organization
    - Install technologies correctly
    - Secure buildings and specified areas / rooms
    - Train staff
    - Audit controls are in place / followed



Policy and Procedures

Table of Contents

33

33

HIPAA Security Risk Analysis (SRA)

- §164.308(a)(1)(ii)(A) Risk analysis (Required): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity or business associate

34

34

SRA - Methodology

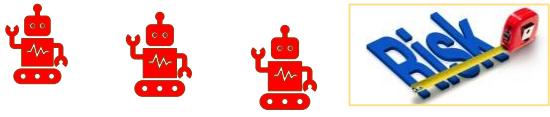
- No single method or "best practice" that guarantees compliance
- Most risk analysis and risk management processes have steps in common:
  - Review existing infrastructure against legal requirements and industry best practices
  - Identify potential vulnerabilities and threats
  - Assesses the impact
  - Prioritize risks

35

Resources: CMS/OCR Security Risk Analysis Tip sheet 12/2013 ,and https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es

35

SRA - Methodology



- Identify where ***all*** ePHI is created, received, maintained, and transmitted
- Review and document what controls your organization has in place to protect the confidentiality, integrity, and availability of ***all*** ePHI

36

Source: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es

36

SRA – Review

- Review and document controls for all HIPAA Security Rule requirements
  - General rules
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
  - Organizational requirements
  - Policies and procedures and documentation requirements

37

37

SRA – Threats and Weaknesses

- Determine what potential risks and vulnerabilities exist that may impact the confidentiality, integrity, and availability of ePHI
  - Threat sources
  - Weaknesses
- Rank them (likelihood and impact)
- Prioritize them

38

38

SRA - Action Plan

- HIPAA Security Rule:
  - §164.308(a)(1)(ii)(B) Risk management (Required): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)
- Create an action plan to address identified risks
- Examples:
  - Core security policies and procedures
  - Correct/update processes
  - Missing technical security controls
  - Monitoring
  - Update software
  - Training

39

39

SRA – Address Risks

- Mitigate risks
- Document actions taken
  - On an action plan
  - In minutes

40

40

SRA Ongoing Efforts: Rinse & Repeat

- HIPAA Security Rule:
  - §164.308(a)(8) Evaluation (Required): Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of ePHI, that establishes the extent to which an entity's security P&Ps meet the requirements of this subpart
- Full HIPAA Security Risk Analysis: on a regular basis (e.g. annually)
  - Review all technologies/systems that create, receive, maintain, or transmit ePHI
  - Review P&Ps
- Complete "mini" risk assessments when purchasing and installing new and updated hardware and software

41

41

Training…Training…Training

- Explain what workforce need to do to protect PHI, such as:
  - Lock unattended workstations
  - Do not provide your user name and password to anyone
  - Do not save PHI on laptops, computers, smart phones
  - Lock PHI in cabinets/offices when not in use & after hours
- Provide examples of incidents and what to report
- Cover all P&Ps that apply to them
- Include the name and contact information of your Security Official / Officer

42

42

Be honest…

Do you feel like this?

43

Or this?

44

Do not feel like you are alone

Talk to your colleagues

Talk to your neighbor
(not about PHI though)

Talk to your coworkers

Join networking groups

45

Take it one step at a time

Do not attempt this alone!

46

46

Resources

- HIPAA Collaborative of Wisconsin http://hipaacow.org
- American Health Information Management Association (AHIMA) http://www.ahima.org/resources/
- Healthcare Information and Management Systems Society www.himss.org
- HCPRO HIPAA Update Blog http://blogs.hcpro.com/hipaa/
- NIST Special Publications (800 series) http://csrc.nist.gov/publications/PubsSPs.html

47

47

Resources

- HHS / OCR HIPAA information http://www.hhs.gov/hipaa/for-professionals/index.html
- Summary of the Security Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
- Security Rule Guidance Material http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
- Guidance on Risk Analysis https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es
- HHS Frequently Asked Questions: http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html
- OCR Enforcement http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html

48

Questions?

49

Holly Schlenvogt

Privacy & Security Consultant / Owner
HRT Consulting, LLC
(262) 468-4291 (Office)
hschlenv@hrt-consulting.com

Thank you!

http://hrt-consulting.com

50