CYBERSECURITY

Recent OCR Actions & Cyber Awareness Newsletters

Claire C. Rosston

HOLLAND&HART

DISCLAIMER

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.

SOURCES

1. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements
2. https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html?language=es
3. https://www.hhs.gov/hipaa/for-professionals/security/index.html

AGENDA

Security traps demonstrated by recent OCR settlements and penalties

Focus: Improving your risk assessment

OCR guidance on mobile devices

OCR guidance on man-in-the-middle (MITM) attacks

RECENT OCR ACTIONS

FRESENIUS MEDICAL CARE NORTH AMERICA

February 1, 2018: $3.5 million settlement and corrective action plan

Laptops, desktops and a USB drive, some of which were unencrypted, were stolen or lost in 5 incidents over 6 months (521 ePHI records)

HHS OCR's findings of HIPAA violations

- Inadequate risk assessment
- Unauthorized access
- Failed to implement policies and procedures regarding:
  - Safeguarding its facilities and equipment from unauthorized access, tampering and theft
  - Receipt and removal of hardware and electronic media containing ePHI
  - Mechanism to encrypt and decrypt ePHI
  - Addressing security incidents
  - Use and access of workstations containing ePHI

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/FMCNA/index.html

FRESENIUS MEDICAL CARE NORTH AMERICA

Corrective action plan requires Fresenius to:

- Complete a risk analysis and risk management plan
- Develop policies and procedures to regularly evaluate environmental or operational changes affecting the security of ePHI
- Implement encryption of hardware and electronic media
- Revise policies and procedures regarding:
  - Receipt and removal of hardware and electronic media
  - Physical access to electronic information systems and facilities
- Augment existing mandatory workforce training program
- Submit to HHS OCR reports on encryption and training as well as annual reports

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/FMCNA/index.html

21ST CENTURY ONCOLOGY, INC.

December 28, 2017: $2.3 million settlement and corrective action plan

Unauthorized access to network database through remote desktop protocol (2,213,597 ePHI records)

HHS OCR's findings of HIPAA violations

- Inadequate risk assessment
- Insufficient security measures
- Failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports
- Disclosed ePHI to third party vendors without BAAs

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/21CO/index.html

21ST CENTURY ONCOLOGY, INC.

Corrective action plan requires 21st Century to:

- Complete a risk analysis and risk management plan
- Revise policies and procedures
- Educate its workforce on policies and procedures
- Provide list of all business associates and copies of all maintained BAAs to HHS OCR
- Set up an internal monitoring plan for compliance with settlement requirements
- Hire third party assessor to review compliance at least annually
- Set up an internal reporting system for all workforce to report violations of HIPAA policies and procedures
- Submit annual reports to HHS OCR

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/21CO/index.html

OTHER OCR ACTIONS IN 2017

$2.5 million settlement for insufficient risk analysis and risk management plan and draft policies and procedures (CardioNet)

$400,000 settlement for delayed and insufficient risk analysis (Metro Community Provider Network)

$5.5 million settlement for failure to implement workforce access policies and procedures and audit controls (Memorial Healthcare System)

$2.3 million penalty for ineffective physical controls and no risk management plan (Children's Medical Center of Dallas)

$2.2 million settlement for no risk analysis or risk management plan and delayed corrective measures (MAPFRE Life Insurance of Puerto Rico)

Other smaller settlements for no BAA and untimely breach notification

Source: https://www.hhs.gov/ocr/newsroom/

IMPROVING YOUR RISK ANALYSIS

HOLLAND&HART

HIPAA SECURITY RULE

General requirements:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains or transmits

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information

(3) Protect against any reasonably anticipated unauthorized uses or disclosures of such information

(4) Workforce compliance

HIPAA SECURITY RULE

Requires compliance with security standards and required and addressable implementation specifications

Flexible approach:

- (1) May choose security measures that are reasonable and appropriate
- (2) Factors to consider:
  - size, complexity and capabilities
  - technical infrastructure, hardware and software security capabilities
  - costs of security measures
  - probability and criticality of potential risks to ePHI

HIPAA SECURITY RULE

Requires regular review and modification of security measures

Requires documenting actions, activities, assessments, policies and procedures in writing

- Retain for 6 years
- Make available to people implementing procedures
- Review periodically and update as needed

ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)

Source: https://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-part164-subpartC-appA.pdf

PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

Source: https://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-part164-subpartC-appA.pdf

TECHNICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

Source: https://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-part164-subpartC-appA.pdf

Security Risk Assessment Tool

- https://www.healthit.gov/providers-professionals/security-risk-assessment-tool
- Windows and iPad version
- Paper versions
- User guide
- 156 questions
- No guarantee of compliant results
- Can document answers, comments and plans in tool

HHS - Risk Assessment Tool

Security Risk Assessment Tool

Tutorial

Current User: none | Logout | www.HealthIT.gov

Users | About Your Practice | Business Associates | Asset Inventory

First Name | Last Name | Initials

Security Risk Assessments

The HIPAA Security Rule requires covered entities to conduct a risk assessment to identify risks and vulnerabilities to electronic protected health information (e-PHI). Risk assessment is the first step in an organization's Security Rule compliance efforts. Following HIPAA risk assessment guidelines will help you establish the safeguards you need to implement based on the unique circumstances of your health care practice.

Risk assessment is an ongoing process that should provide your medical practice with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI. HIPAA requires that covered entities "implement policies and procedures to prevent, detect, contain, and correct security violations" by conducting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the [organization]." Performing a security risk assessment and mitigating the findings is also a requirement for providers attesting to "Meaningful Use" under the CMS EHR Incentive Program.

Providers should develop a risk assessment that addresses these criteria by evaluating the impact and likelihood of potential breaches, implementing security features, cataloguing security features, and maintaining security protections.


HHS - Risk Assessment Tool
Security Risk Assessment Tool
Tutorial
Current User: cms | Logout | www.HealthIT.gov
A57
§164.308(a)(8) - Standard
Does your practice maintain and implement policies and procedures for assessing risk to ePHI and engaging in a periodic technical and non-technical evaluation in response to environmental or operational changes affecting the security of your practice's ePHI?
Yes No Flag
Which best explains your reason for answering NO:
Cost Practice Size Complexity Alternate Solution
Current Activities
Notes
Remediation
With respect to a threat/vulnerability affecting your ePHI:
Likelihood: Low Medium High
Impact: Low Medium High
Previous Question
Next Question
Things to Consider
Threats and Vulnerabilities
Examples of Safeguards
Your practice may not be able to safeguard its ePHI against risks due to environmental and operational changes if it does not engage in periodic evaluations, both technical and non-technical.
Some potential impacts include:
· Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your practice's ePHI.
· Unauthorized disclosure, loss, or theft of ePHI can lead to medical identity theft.
· Accurate ePHI may not be available when needed, which can adversely impact your healthcare professionals' ability to diagnose and treat their patients.
Report
Glossary
Navigator
Related Info
Export

NIST 800-30: RISK ASSESSMENT

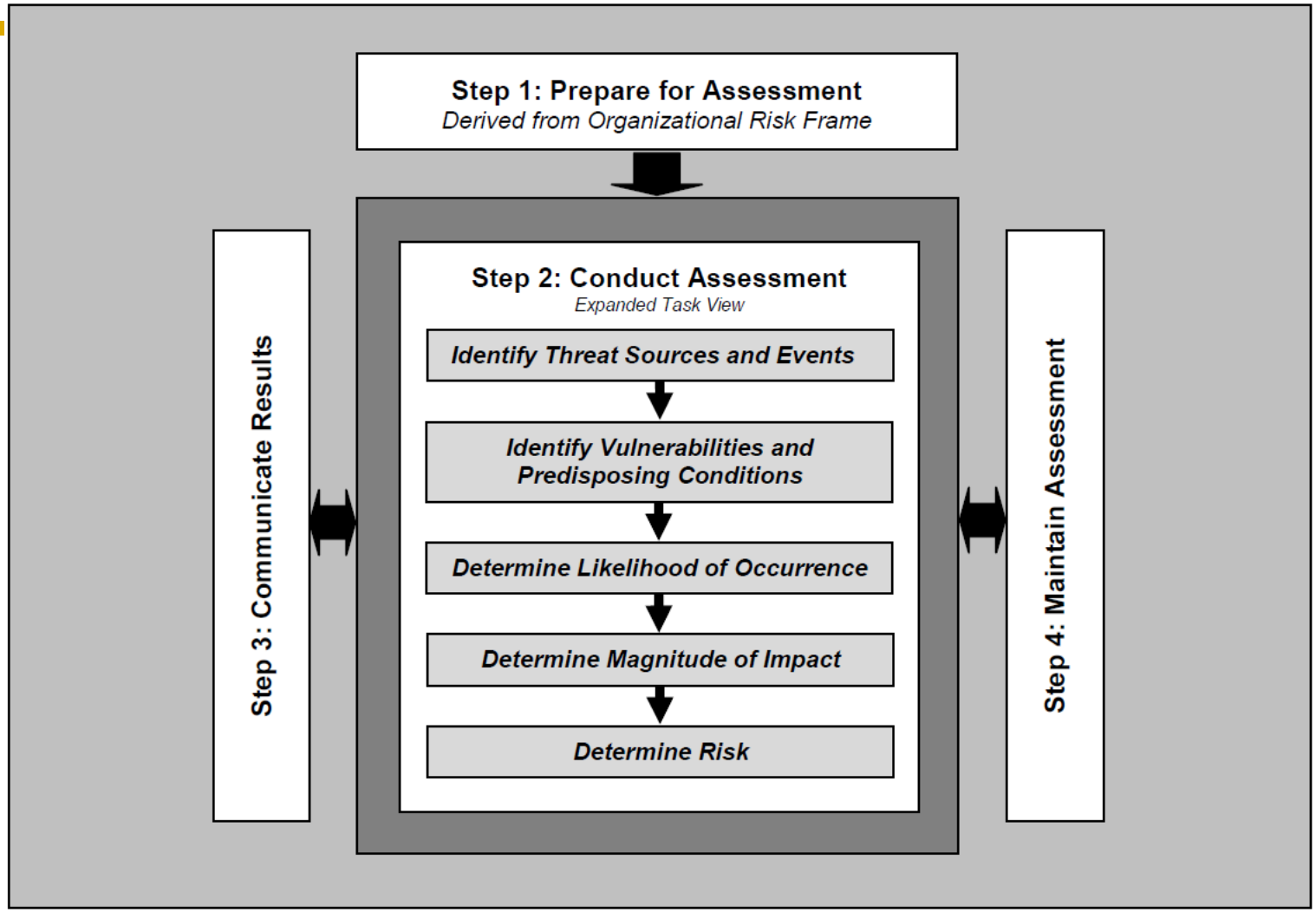

FIGURE 5: RISK ASSESSMENT PROCESS

Source: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

VULNERABILITIES

Flaws or weaknesses in system security procedures, design, implementation or internal controls

- Technology: bugs, misconfiguration, inherent weakness
- People: social engineering, poor choices
- Process: defects, data handling

ePHI records for sale:

- Russian-speaking hacker is offering access to 2 medical offices (15,000 New York patient records and 11,000 Michigan patient records)
- Both offices use eClinicalWorks software but hacker claims access was obtained via compromised virtual network computing (VNC) protocol

Sources of Known Vulnerabilities

US-CERT	• https://www.us-cert.gov/mailing-lists-and-feeds
CVE: Common Vulnerabilities and Exposures	• https://cve.mitre.org/index.html
NVD: National Vulnerability Database	• https://nvd.nist.gov/

RISK ASSESSMENT

Common Mistakes:

- Failure to account for third-party risk
  - SAAS, Cloud, Business Associates
  - Right to audit over-reliance in absence of SOC 2
  - Misunderstanding of SOC 1 vs. SOC 2 reports
- Failure to completely inventory ePHI and systems
- Not conducting a risk assessment as defined, opting for gap analysis
- No risk assessment at all
- No minutes of board deliberations or documentation of management action

ACTION ITEMS

When you return to work:	• Identify when your next risk assessment is due • Review last risk assessment • Identify shortcomings
30 days:	• Discuss noted shortcomings with management • Assign accountable party to plan for upcoming risk assessment to address observed weaknesses, based on OCR guidance
90 days:	• Complete inventory of: ePHI, storage media, transmission, systems and endpoints
180 days:	• Conduct an improved risk assessment

RECENT OCR NEWSLETTERS

MOBILE DEVICES

Risks

- Greater risk of being lost or stolen
- Unsecure settings and connectivity

If devices are not allowed to be used for activities involving ePHI, develop and implement policies and procedures that make this prohibition clear

MOBILE DEVICES

Properly configure and secure devices

- Consider using Mobile Device Management (MDM) software to manage and secure mobile devices
- Install or enable automatic lock/logoff functionality
- Require authentication to use or unlock mobile devices
- Install or enable encryption, anti-virus/anti-malware software and remote wipe capabilities
- Use only secure Wi-Fi connections
- Use a secure Virtual Private Network (VPN)

MOBILE DEVICES

- Regularly install security patches and updates
- Consider using Mobile Device Management (MDM) software to manage and secure mobile devices
- Use a privacy screen to prevent people close by from reading information on your screen
- Reduce risks posed by third-party apps by prohibiting the downloading of third-party apps, using whitelisting to allow installation of only approved apps, securely separating ePHI from apps and verifying that apps only have the minimum necessary permissions required
- Train workforce on how to securely use mobile devices
- Securely delete all ePHI stored on a mobile device before discarding or reusing the mobile device

MAN-IN-THE-MIDDLE ATTACKS

MITM attacks: third party intercepts communications (e.g., ePHI) and may alter information or inject malicious code

Some organizations use Secure Hypertext Transport Protocol (HTTPS) for end-to-end connection security and HTTPS interception products to detect malware over the HTTPS connection

Many HTTPS interception products are inadequate (see https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html for partial list)

Use https://badssl.com/ to determine if your HTTPS interception product is inadequate

See US-CERT's other recommendations regarding MITM attacks at https://www.us-cert.gov/ncas/alerts/TA15-120A

THANKS FOR COMING!

Claire C. Rosston

ccrosston@hollandhart.com

HOLLAND&HART