




HIPAA SECURITY RULE

Recent OCR Actions,
Risk Assessments,
& Hot Topics

Matt Sorensen

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. Dept. of Health and Human Services, HIPAA Security Series, Volume 2, Paper 6: Basics of Risk Analysis and Risk Management,
<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf>. Last accessed 12/19/2016.
2. <https://www.healthit.gov/providers-professionals/security-risk-assessment>. Last accessed 12/19/2016.

AGENDA

- Security traps demonstrated by recent OCR settlements
- Performing and documenting a risk assessment
- Required safeguards: what you really need to address
- To encrypt or not to encrypt: mobile devices, e-mails, texts and other communications
- OCR guidance concerning cloud computing, ransomware, and other items




RECENT OCR ACTIONS

CHILDREN'S MEDICAL CENTER OF DALLAS

- February 2, 2017: \$3.2 Million Fine
- Lost Blackberry in 2010 (3,800 ePHI records)
- Lost laptop in 2013 (2,462 ePHI records)
- “impermissible disclosure of unsecured (ePHI) and non-compliance over many years with multiple standards of the HIPAA Security Rule.”
 - Lack of risk management plans
 - No encryption on mobile devices
 - Ineffective physical access controls

Sources:

<https://www.hhs.gov/about/news/2017/02/01/lack-timely-action-risks-security-and-costs-money.html>

<http://www.healthcareitnews.com/news/ocr-fines-childrens-medical-center-dallas-32-million-lack-encryption>

<https://www.hhs.gov/sites/default/files/childrens-notice-of-proposed-determination.pdf>

CHILDREN'S MEDICAL CENTER OF DALLAS

- Notice of Proposed Determination
 - No Request for Hearing
 - “opportunity to provide written evidence of mitigating factors or affirmative defenses and/or written evidence in support of a waiver of a [civil monetary penalty]”
- Aggravating Factors
 - continued use of unencrypted devices from 2008 to 2013
 - prior history of non-compliance
 - losses of laptop, blackberry put them on notice of active risk of compromise of ePHI and non-compliance
 - Reportable incidents in 2008, 2009, 2010, 2013

MAPFRE LIFE INSURANCE OF PUERTO RICO

- January 18, 2017: \$2.2 Million Fine
- “With this resolution amount, OCR balanced potential violations of the HIPAA Rules with evidence provided by MAPFRE with regard to its present financial standing.”
- Stolen USB memory stick, 2011 (2,209 ePHI records)

Sources:

<https://www.hhs.gov/about/news/2017/01/18/hipaa-settlement-demonstrates-importance-implementing-safeguards-ephi.html>

MAPFRE LIFE INSURANCE OF PUERTO RICO

- “Failure to conduct its risk analysis and implement risk management plans, contrary to its prior representations, and a failure to deploy encryption or an equivalent alternative measure on its laptops and removable storage media until September 1, 2014.
- “MAPFRE also failed to implement or delayed implementing other corrective measures it informed OCR it would undertake.”

OTHER OCR ACTIONS

- \$475,000 for lack of timely breach notification (Presence Health)
- \$400,000 for failure to update BAA for over ten years (CARE New England Health System)
 - “WIH failed to renew or modify its existing written business associate agreement with Care New England Health System, its business associate, to include the applicable implementation specifications required by the Privacy and Security Rules.”
- \$2.75 Million (University of Mississippi Med Center)
 - breach of ePHI of “10,000 individuals. During the investigation, OCR determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, yet no significant risk management activity occurred until after the breach, due largely to organizational deficiencies and insufficient institutional oversight.”

Sources:

<https://www.hhs.gov/ocr/newsroom/>

<https://www.hhs.gov/sites/default/files/9-14-16-wih-racap-1.pdf>

OTHER OCR ACTIONS


- \$2.7 Million
 - lost laptop (4,022 ePHI records)
 - lack of BAA with third-party cloud storage provider who suffered a breach (3,044 ePHI records)
- How many improvements could you make with \$2.7 million?
 - “We made significant data security enhancements at the time of the incidents and now are investing at an unprecedented level in proactive measures to further safeguard patient information,” Barnes continued. “In the face of these challenges, OHSU is proactively working to ensure the creation of a sustainable gold standard for protected health information security and HIPAA compliance.”

Sources:

<https://www.hhs.gov/ocr/newsroom/>

SUMMARY OF RECENT ISSUES

- Missing or outdated BAAs
- Missing or inadequate risk assessment
- Failure to act in the face of known risks
 - failure to encrypt
 - failure to restrict access (physical & logical)
- Failure to perform timely breach notification
- Failure to respond to OCR Notice of Determination



PERFORMING &
DOCUMENTING
THE RISK ASSESSMENT

HIPAA SECURITY RULE

- 45 CFR 164.302-318
- 164.306 (General Requirements)
 - (a)(1) Ensure the confidentiality, integrity, and availability of all **electronic protected health information** the covered entity or business associate creates, receives, maintains, or transmits.
 - (a)(2) Protect against any reasonably anticipated threats or hazards to the **security** or **integrity** of such information.
 - (a)(3) Protect against any reasonably anticipated **uses** or **disclosures** of such information

HIPAA SECURITY RULE

- **164.306 (General Requirements)**
 - (b) Flexibility of Approach
 - Choose Security Measures That Are **Reasonable & Appropriate**
 - How do we know what is Reasonable & Appropriate?
 - size and complexity
 - technical infrastructure, hardware, and security capabilities
 - cost of security measures
 - **probability** and **criticality** of potential risks to ePHI
 - (c) Standards
 - (d) Implementation Specifications

HIPAA SECURITY RULE

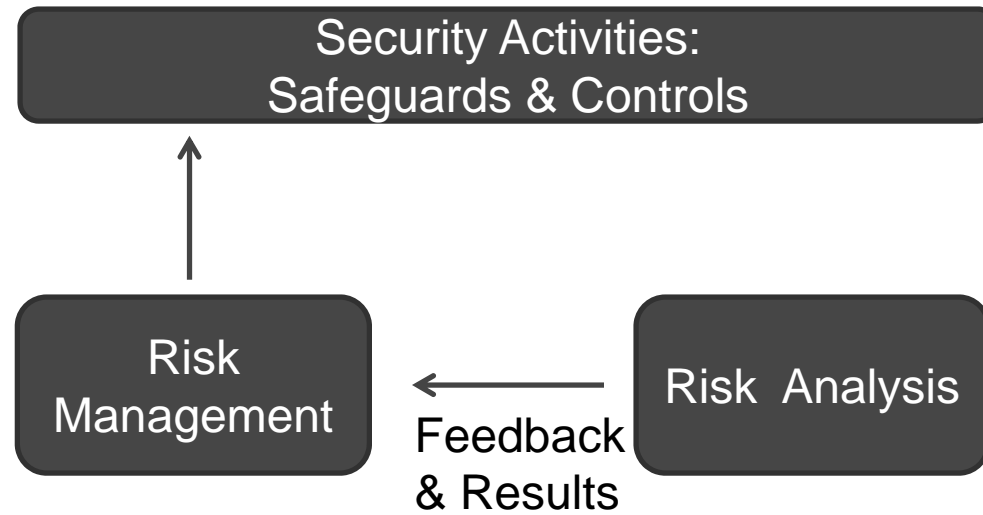
- 164.308 (Administrative Safeguards)
 - (a)(1)(i) Standard: Security Management Process
 - Implement policies and procedures to prevent, detect, contain, and correct security violations.
 - (a)(1)(ii) Implementation Specifications:
 - (ii)(A) Risk Analysis: Conduct an accurate and thorough **assessment** of the **potential risks** and **vulnerabilities** to the confidentiality, integrity and availability of electronic protected health information.
 - (ii)(B) Risk Management: Implement security measures sufficient to **reduce risks and vulnerabilities** to a reasonable and appropriate level to comply with § 164.306(a).

HIPAA SECURITY RULE - DOCUMENTATION

- 164.316(B)(1)(ii):
If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

ID	Risk Assessment Project																		
1	1 System Documentation Phase	←→																	
2	1.0 Set boundary for selected system	█																	
3	1.1 Record system identification information	█																	
4	1.2 Document system purpose and desc.	█																	
5	1.3 Document the system security level	█																	
6	2 System Risk Determination Phase	←→																	
7	2.1 Identify threats and vulnerabilities	█																	
8	2.2 Describe risks	█																	
9	2.3 Identify existing controls	█																	
10	2.4 Determine likelihood of occurrence	█																	
11	2.5 Determine severity of impact	█																	
12	2.6 Determine risk levels	█																	
13	3 Safeguard Determination Phase	←→																	
14	3.1 Recommend controls and safeguards	█																	
15	3.2 Determine residual likelihood of occurrence	█																	
16	3.3 Determine residual severity of impact	█																	
17	3.4 Determine residual risk level	█																	
18	4 Report presentation, archiving and sign-off	█																	

RISK MANAGEMENT & ANALYSIS



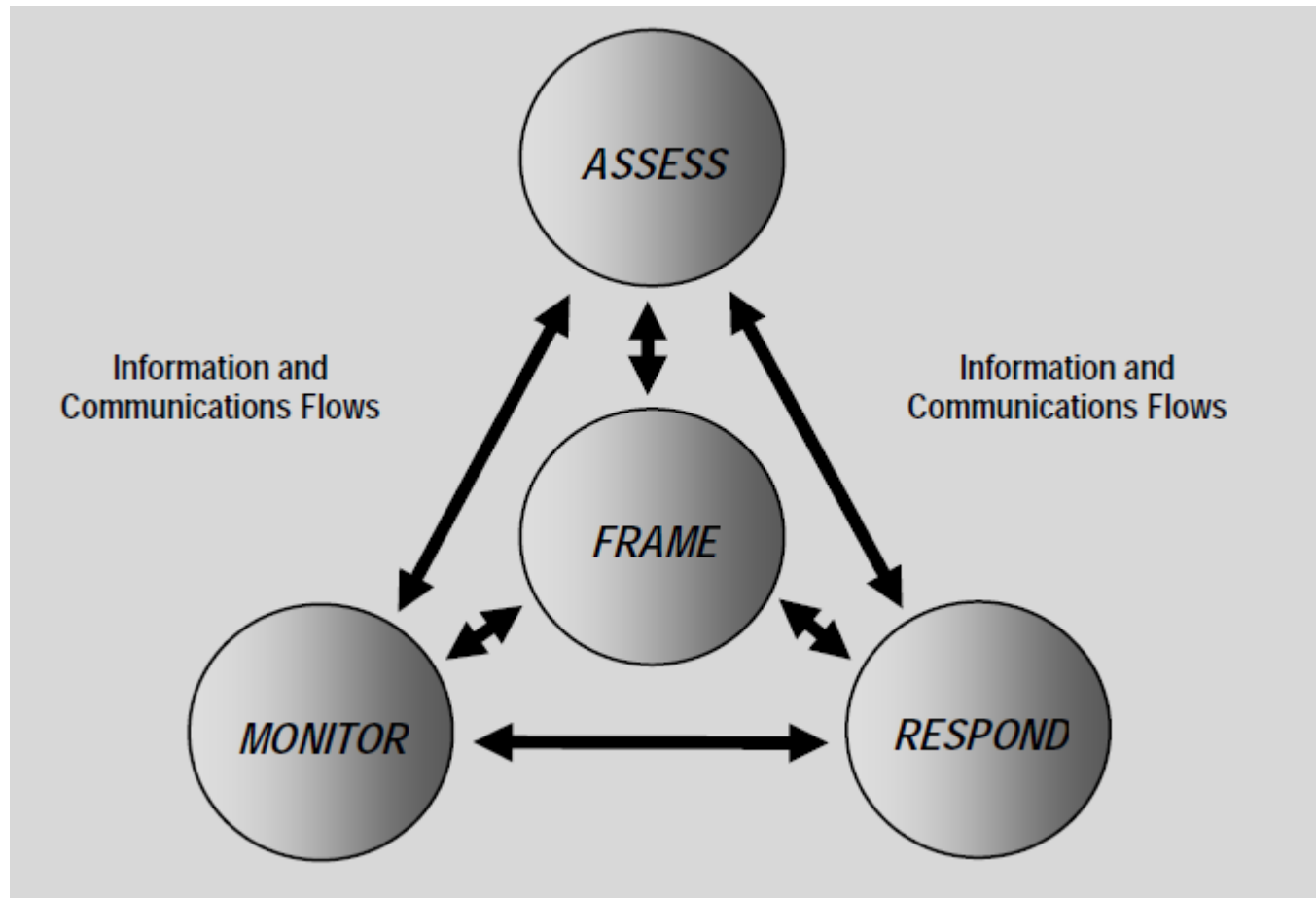
NIST STANDARDS

“Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization’s implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.” – Source: CMS FAQ on Security Rule.

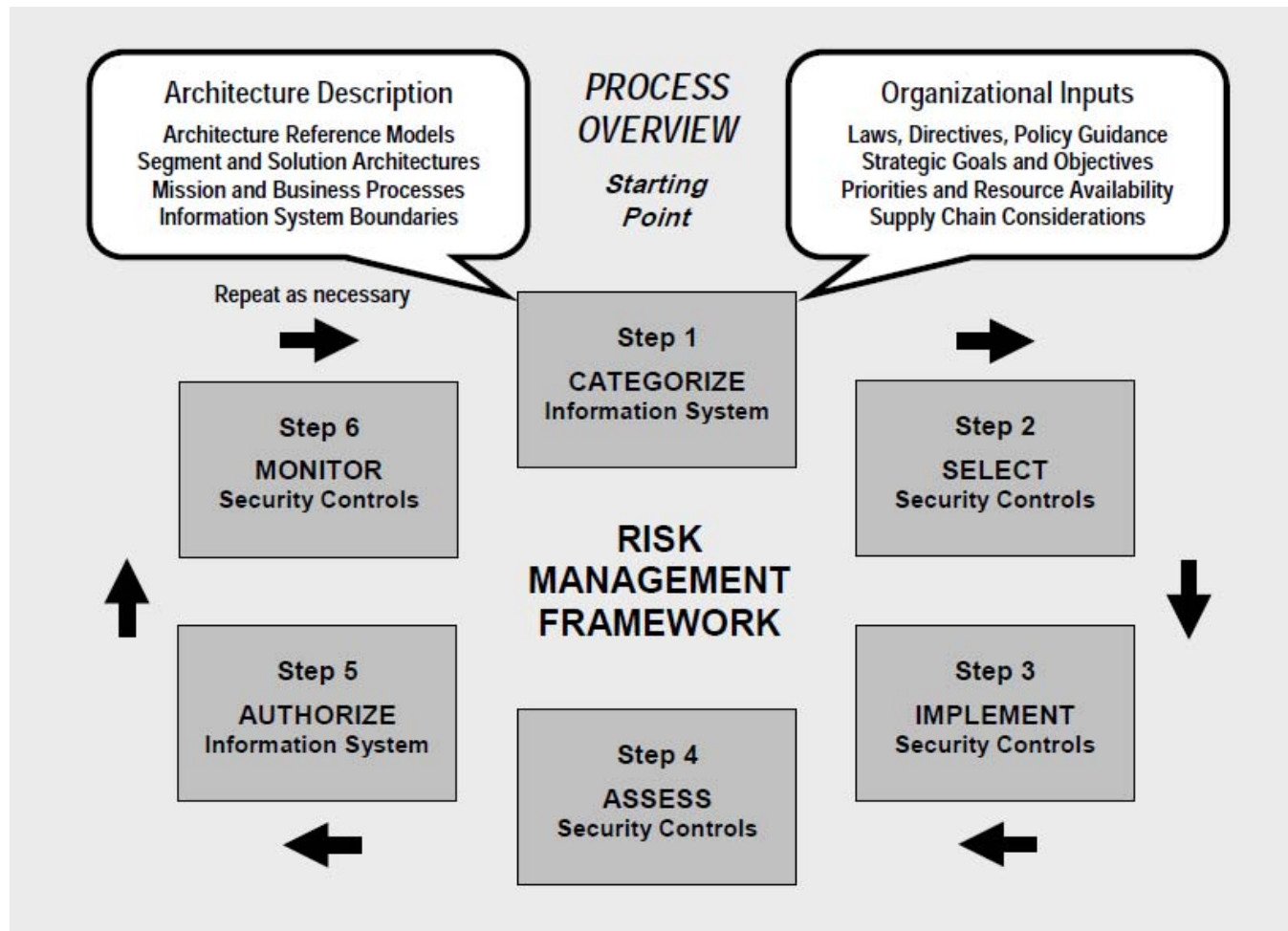
NIST STANDARDS

- **800-39: Managing Information Security Risk**
- **800-37: Risk Management Framework**
- **800-30: Risk Assessment**

NIST 800-39: MANAGING INFORMATION SECURITY RISK



NIST 800-37: RISK MGMT FRAMEWORK



NIST 800-30: RISK ASSESSMENT

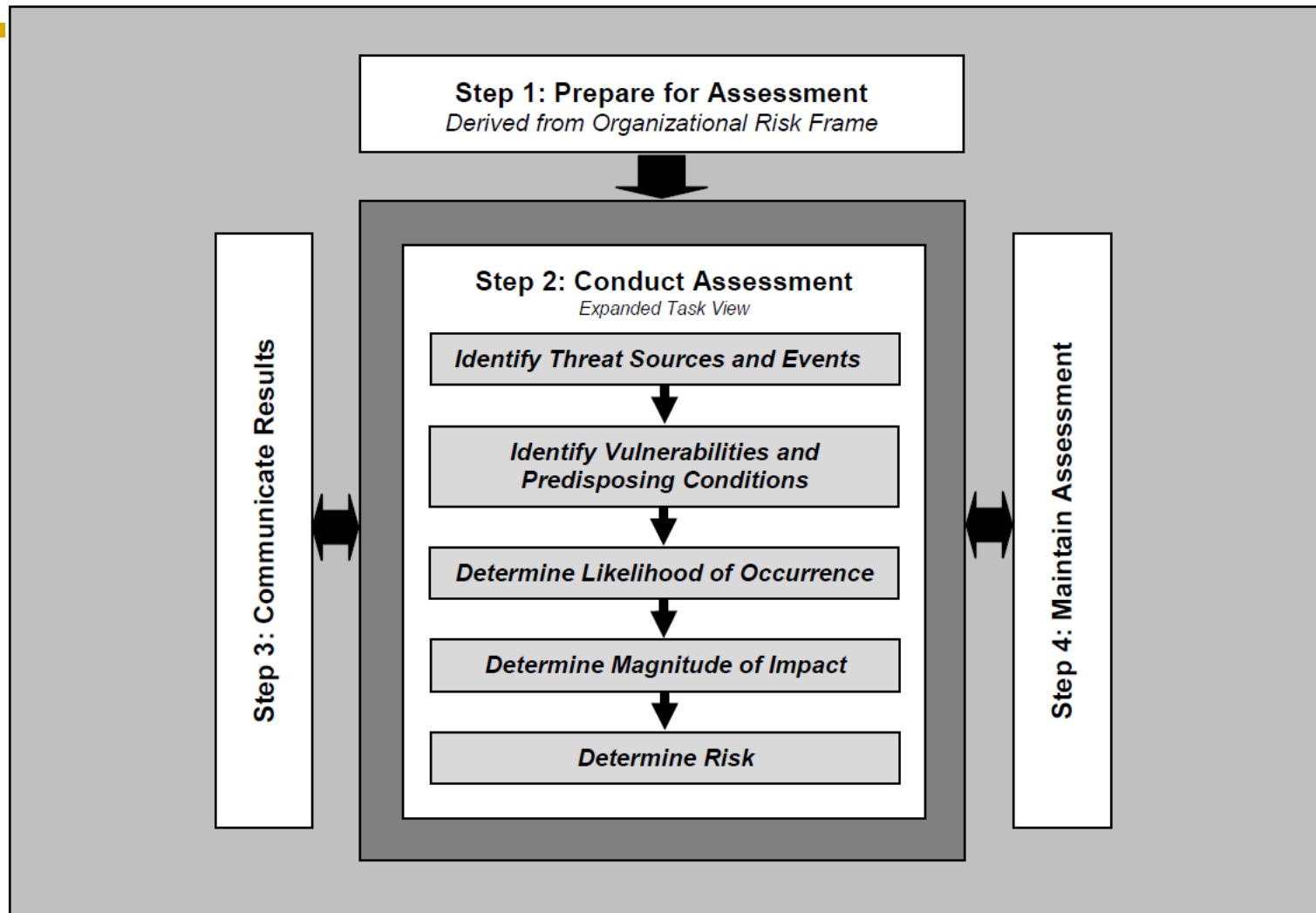
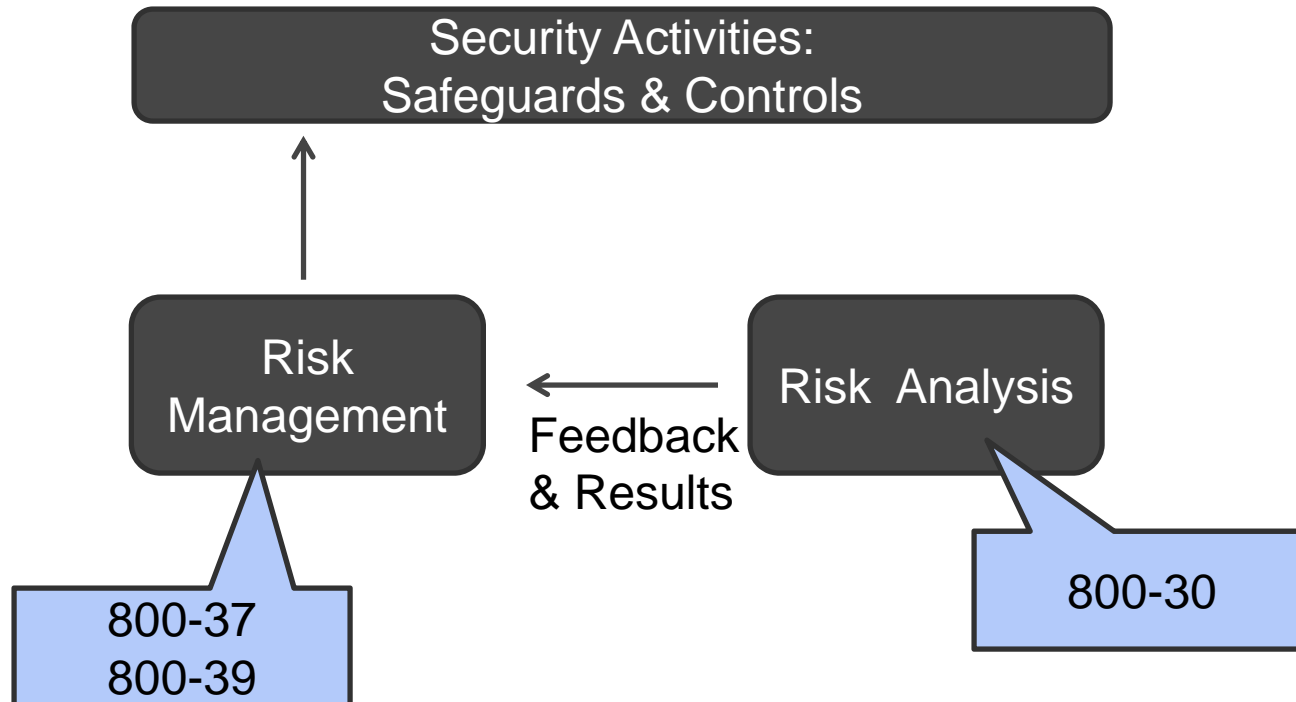


FIGURE 5: RISK ASSESSMENT PROCESS

RISK MANAGEMENT & ANALYSIS



RISK DEFINITIONS

- **Vulnerability:** “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised”
- **Threat:** “[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”
- **Risk:** “The net mission impact considering (1) the *probability* that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting *impact* if this should occur.

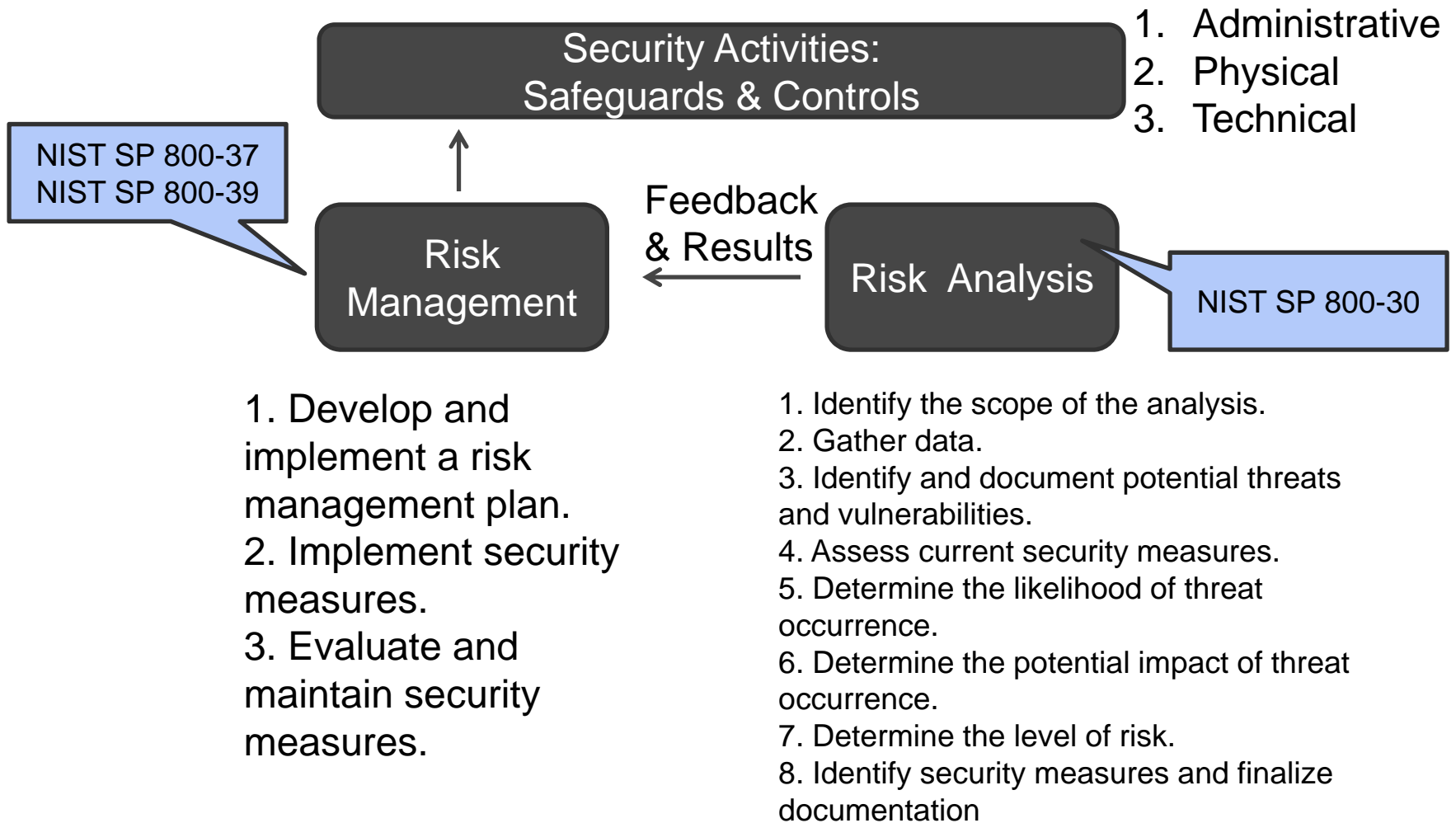
RISK DEFINITIONS (SIMPLIFIED)

- **Vulnerability:** a flaw or weakness.
- **Threat:** potential of a person or thing to exercise a vulnerability.
- **Risk:** The combination* of the likelihood and impact of a threat exploiting a vulnerability.
 - *Could also be:
 - function of
 - estimation of
 - cross-section of
 - calculation of
 - prognostication about
 - reasonable belief in, (based on experience, recent trends, and foreseeability)

RISK ASSESSMENT TERMS– EXAMPLES

- **Threats -> Vulnerabilities = Risk**
 - **Threat Analysis**
 - Human: intentional & unintentional
 - Natural: natural disaster
 - Environmental: power failures, chemical/pollutant
 - **Vulnerabilities**
 - in Technology: bugs, misconfiguration, inherent weakness
 - in People: social engineering, poor choices
 - in Process: defects, data handling

RISK MANAGEMENT & ANALYSIS



RISK ANALYSIS STEPS

Risk Analysis

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

RISK ANALYSIS STEPS

Risk Analysis

1. **Identify the scope of the analysis**
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

RISK ASSESSMENT - SCOPE

- Includes potential risks and vulnerabilities to:
 - confidentiality,
 - availability, and
 - integrity of
- all ePHI that a covered entity creates, receives, maintains, or transmits.
- Includes ePHI in all forms of electronic media:
 - storage
 - network transmission

Risk Analysis

1. Identify the scope of the analysis
2. **Gather data**
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

RISK ASSESSMENT - TECHNIQUES

- **Gather Data**
 - Inventory of ePHI
 - Inventory of Systems
 - Workstations
 - Laptops
 - Mobile Devices
 - Servers and Databases
 - Interviews, Documentation, Past Projects

RISK ANALYSIS STEPS

Risk Analysis

1. Identify the scope of the analysis
2. Gather data
3. **Identify and document potential threats and vulnerabilities**
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

RISK ASSESSMENT - TECHNIQUES

- **Threats -> Vulnerabilities = Risk**
 - **Threat Analysis**
 - **Human: SKRAAMO**
 - nation state
 - organized crime
 - hacktivist
 - opportunist
 - insider threats
 - **Natural: regional occurrences**
 - **Environmental: proximity to industry**

RISK ASSESSMENT - TECHNIQUES

- **Threats -> Vulnerabilities = Risk**
 - **Vulnerability Management: Find & Fix**
 - in Technology: Scan, Review
 - in People: Assess Knowledge, Practices
 - in Process: Audit, Design, Effectiveness

ASSESSING EXPLOITABILITY WITH COMMON VULNERABILITY SCORING SYSTEM (CVSS)

- A vulnerability assessment tool or similar scoring system to rate vulnerabilities and determining the need for an urgency of the response.
- **Base Scoring (risk factors for vulnerability)**
 - Attack Vector (physical, local, adjacent, network)
 - Attack Complexity (high, low)
 - Privileges Required (none, low, high)
 - User Interaction (none, required)
 - Scope (changed, unchanged)
 - Confidentiality Impact (high, low, none)
 - Integrity Impact (none, low, high)
 - Availability Impact (high, low, none)
- **Temporal Scoring (risk factors that change over time)**
 - Exploit Code Maturity (high, functional, proof-of-concept, unproven)
 - Remediation Level (unavailable, work-around, temporary fix, official fix, not defined)
 - Report Confidence (confirmed, reasonable, unknown, not defined)

CVSS – Common Vulnerability Scoring System
https://www.first.org/cvss/cvss_basic-2.0.pdf.

POPULAR EMR PROVIDERS



Sales +1 866 643 8367 | [Log In](#)

Solutions ▾

Pricing

Company ▾

Resources ▾

[Request Demo](#)



SOURCES OF KNOWN, PUBLISHED VULNERABILITIES

- CVE: Common Vulnerabilities and Exposures
 - <https://cve.mitre.org/cve/cve.html>
- National Vulnerability Database
 - <https://nvd.nist.gov/>

RISK ANALYSIS STEPS

Risk Analysis

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. **Assess current security measures**
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

RISK ASSESSMENT – ASSESS SAFEGUARDS

- **Safeguards (Controls)**
- **Preventive, Corrective, Detective**
- **Manual, Automated, Hybrid**
- **Test of Design**
 - Is the safeguard designed properly to detect what it purports to detect?
- **Test of Effectiveness**
 - Inspect, Duplicate, Feed known bad events, Sample

RISK ANALYSIS STEPS

Risk Analysis

1. Identify the scope of the analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the **likelihood** of threat occurrence
6. Determine the potential **impact** of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

EXAMPLE: ASSESSING SEVERITY OF PATIENT HARM (FDA MED DEVICE GUIDANCE)

Common Term	Possible Description
Negligible	Inconvenience or temporary discomfort
Minor	Results in temporary injury or impairment not requiring professional medical intervention
Serious	Results in injury or impairment requiring professional medical intervention
Critical	Results in permanent impairment or life-threatening injury
Catastrophic	Results in patient death

ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices – 441 Application of Risk Management to Medical Devices:

RISK ASSESSMENT

- **Threats -> Vulnerabilities = Risk**
 - **Impact**
 - L/M/H
 - **Dollar Amount**
 - Cost per breached record
 - Cost of breach, # of records
 - **Score**
 - **Likelihood**
 - L/M/H
 - **Quantitative vs. Qualitative**

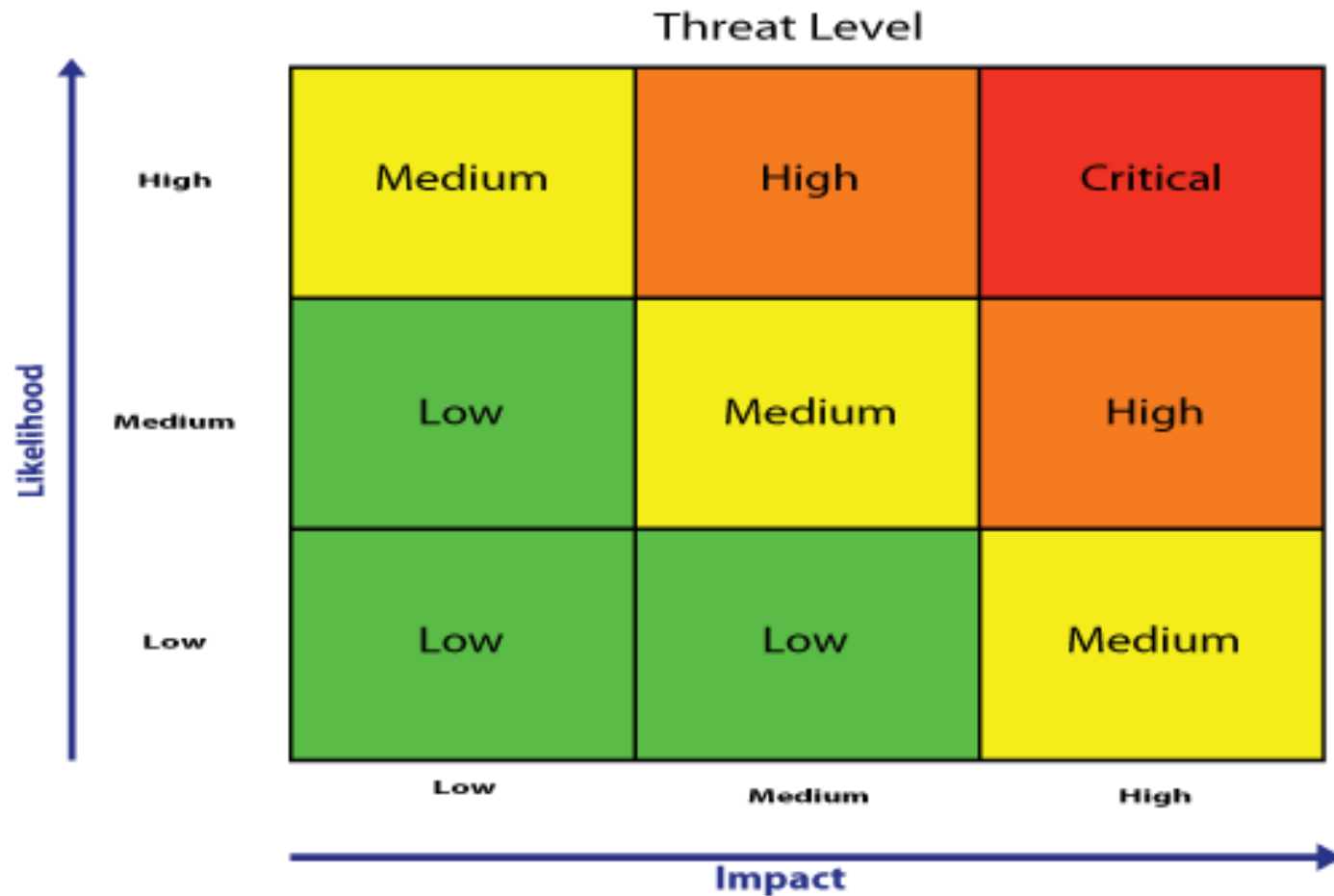
RISK ASSESSMENT – PROBABILITY

- Wall Street Quants
- Wired Magazine Cover 3/09
- Reminder:
 - we are tasked with foreseeing “reasonably anticipated” threats and hazards, uses and disclosures
 - addressing those with reasonable and appropriate safeguards

THE
SECRET FORMULA
That Destroyed Wall Street
 $P = \phi(A, B, \gamma)$

- <https://www.wired.com/2009/02/wp-quant/>
- <http://archive.wired.com/wired/issue/17-03>

RISK LEVEL



EXAMPLE: FDA POSTMARKET MED DEVICE CYBERSECURITY RISK ASSESSMENT



ACTION PLANS

- **Critical**
 - Item 1
 - Solution
 - Cost
 - Due Date
 - Item 1
 - etc.
- **High**
 - Item 3
 - Solution
 - Cost
 - Due Date
 - Item 4
- **Medium**
 - etc.
- **Low**
 - etc.

RISK ASSESSMENT

- What is not considered a risk assessment:
 - Gap Assessment against the implementation specifications
 - A list of threats and corresponding safeguards
 - follow all the steps
 - show deliberation in:
 - identifying all ePHI
 - completing inventories
 - threat identification, likelihood and impact analysis

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 complete and inventory of ePHI and systems
 - Not conducting a risk assessment as defined, opting for gap analysis
 - No risk assessment at all!
 - No minutes of board deliberations, management action

RISK ASSESSMENT TOOL

- **Security Risk Assessment Tool**
 - HealthIT.gov
 - Windows and iPad version
 - Paper versions
 - User guide
 - No guarantee of compliant results

Source: <https://www.healthit.gov/providers-professionals/security-risk-assessment-tool>

RISK ASSESSMENT GUIDANCE

- **Risk Assessment Guidance**
- **Security Risk Assessment Tool**
 - HealthIT.gov
 - Windows and iPad version
 - Paper versions
 - User guide
 - No guarantee of compliant results

Source:

<https://www.healthit.gov/providers-professionals/security-risk-assessment>

<https://www.healthit.gov/providers-professionals/security-risk-assessment-tool>



Security Risk Assessment Tool

Tutorial

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



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.

Users	About Your Practice	Business Associates	Asset Inventory
First Name	Last Name	Initials	



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

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.

Previous Question | Next Question | Report | Glossary | Navigator | Related Info | Export

ACTION ITEMS: 30-90-180

- **When you return to work**
 - Identify when your next risk assessment is due
 - Review last risk assessment
 - Identify shortcomings, gaps
- **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, and systems and endpoints
- **180 days:**
 - Conduct an improved risk assessment



DOCUMENTING
ADDRESSABLE
SAFEGUARDS

APPLYING A “FLEXIBLE APPROACH”

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)
Evaluation	164.308(a)(8)	Applications and Data Criticality Analysis (A) (R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)

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)

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 In-formation (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

ADDRESSABLE

- A covered entity will do one of the following for each addressable specification:
 - (a) implement the addressable implementation specifications; (if it is reasonable and appropriate to do so); OR
 - (b) implement one or more alternative security measures to accomplish the same purpose; (if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative.); OR
 - (c) not implement either an addressable implementation specification or an alternative.

DOCUMENTATION OF DECISIONS

- This decision will depend on a variety of factors such as:
 - the entity's risk analysis,
 - risk mitigation strategy,
 - what security measures are already in place,
 - the cost of implementation.
- The decisions that a covered entity makes regarding addressable specifications must be documented in writing.
- The written documentation should include the factors considered as well as *the results of the risk assessment* on which the decision was based.

DOCUMENTATION OF DECISIONS

- This decision will depend on a variety of factors such as:
 - the entity's risk analysis,
 - risk mitigation strategy,
 - what security measures are already in place,
 - the cost of implementation.
- The decisions that a covered entity makes regarding addressable specifications must be documented in writing.
- The written documentation should include the factors considered as well as *the results of the risk assessment* on which the decision was based.

If only a gap assessment were performed in lieu of a risk assessment, how would that help you justify not addressing an Addressable Safeguard?

SECURITY RULE: FLEXIBILITY

- **164.306 (Security Standards: General Rules)**
 - (b) Flexibility of Approach
 - Choose Security Measures That Are **Reasonable & Appropriate**
 - How do we know what is Reasonable & Appropriate?
 - size and complexity
 - technical infrastructure, hardware, and security capabilities
 - cost of security measures
 - **probability** and **criticality** of potential risks to ePHI




HOT TOPICS

WHAT TO ENCRYPT?

- Whether you encrypt depends on your risk assessment
- However:
 - Failure to encrypt PHI on mobile devices is asking for big trouble
 - Why is PHI on mobile devices in the first place?
 - Document the business reasons, then the risks (threats and vulnerabilities) including impact and likelihood
 - Then document the chosen safeguard: encryption
- PHI at Rest
 - in databases
 - in flat files, spreadsheets,
- PHI in Transit
 - Email (Why is PHI in email? See above)
 - EMR
 - Third Party Service Provider
 - Text Messages (Why is PHI in text messages? See above)

MOBILE DEVICE GUIDANCE

- Five Steps
 1. Decide whether mobile devices will access, transmit or store PHI or function as part of EMR system
 2. Assess the risks (threats and vulnerabilities)
 3. Identify mobile device risk management strategy, including safeguards
 4. Develop, Document, Implement
 5. Train: Security awareness

Source:

<https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security>

66 <https://www.healthit.gov/providers-professionals/five-steps-organizations-can-take-manage-mobile-devices-used-health-care-pro>

WANNACRY RANSOMWARE

- Microsoft CVE-2017-0143
- NSA created EternalBlue tool, later stolen and leaked
- Opportunist Hackers used EternalBlue in WannaCry
- Virus/Worm Hybrid
 - Requires clicked attachment to email
 - Then runs unchecked through the local network
- Inoculation:
 - Patching (Windows Update)
 - Email Filtering (Security Email Gateway)
 - User Awareness
 - Anti-virus
 - Remove admin rights
 - Application Whitelisting

WANNACRY SCREEN SHOT

Wanna Decryptor 1.0

Oops, your files have been encrypted!



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)

You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>. If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Send \$300 worth of bitcoin to this address: [QR Code](#)

 **bitcoin**
ACCEPTED HERE

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1 [Copy](#)

[About bitcoin](#)
[How to buy bitcoins?](#)

[Contact Us](#)

[Check Payment](#) [Decrypt](#)

RANSOMWARE

- “Ransomware infections are security incident under the Security Rule”
- “Once detected the covered entity must initiate its security incident and response and reporting procedures.”
- “Part of a deeper analysis should involve assessing whether or not there was a breach of PHI as a result of the security incident.”
- “The presence of ransomware (or any malware) is a security incident under HIPAA that may also result in an impermissible disclosure of PHI in violation of the Privacy Rule and a breach, depending on the facts and circumstances of the attack.”

Source:
<https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

CLOUD COMPUTING

- Business Associate Agreements
 - Right to audit
 - Attestation Requirements
 - Incident Procedures; Notification Requirements
- Third-Party Risk Management
 - Risk Assessment
 - SOC 2
 - Regular Vulnerability Assessments

**THANKS FOR
COMING!**

Matt Sorensen
cmsorensen@hollandhart.com

