Meaningful Use

Security Risk Analysis

Presented by

HealthTech Solutions

HealthTech Solutions

Meaningful Use Measure 1 – for program year 2016

Meaningful Use Measure 1 is an extension of the privacy protection guaranteed to all Americans under the Health Information Portability and Accountability Act (HIPAA).

The objective of Measure 1 is to protect the electronic health information created or maintained by an Electronic Health Record (EHR) by implementing of appropriate technical safeguards.

To demonstrate compliance with Measure 1, you must:

conduct a security risk analysis of your EHR technology	implement all new security updates	have a process in place for correcting identified technology deficiencies

Agenda

- Objective, Measure, Exclusion
- Attestation Requirements
- Centers for Medicare & Medicaid Services (CMS) Guidance
- Safeguards (Administrative, Technical, Physical)
- Required vs. Addressable
- Security Assessment Tools
- Audits

Objective, Measure, Exclusion

Protect Patient Health Information	
Objective	Protect electronic health information created or maintained by the CEHRT through the implementation of appropriate technical capabilities.
Measure	Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by CEHRT in accordance with requirements under 45 CFR164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process.
Exclusion	No exclusions.

Attestation Requirements

Eligible professionals (EPs) must attest YES to conducting or reviewing a security risk analysis and implementing security updates as necessary and correcting identified security deficiencies to meet this measure.

CMS Guidance

EPs must conduct or review a security risk analysis at least annually

An analysis must be done upon installation or upgrade to a new system

It is acceptable for the security risk analysis to be conducted outside the EHR reporting period.

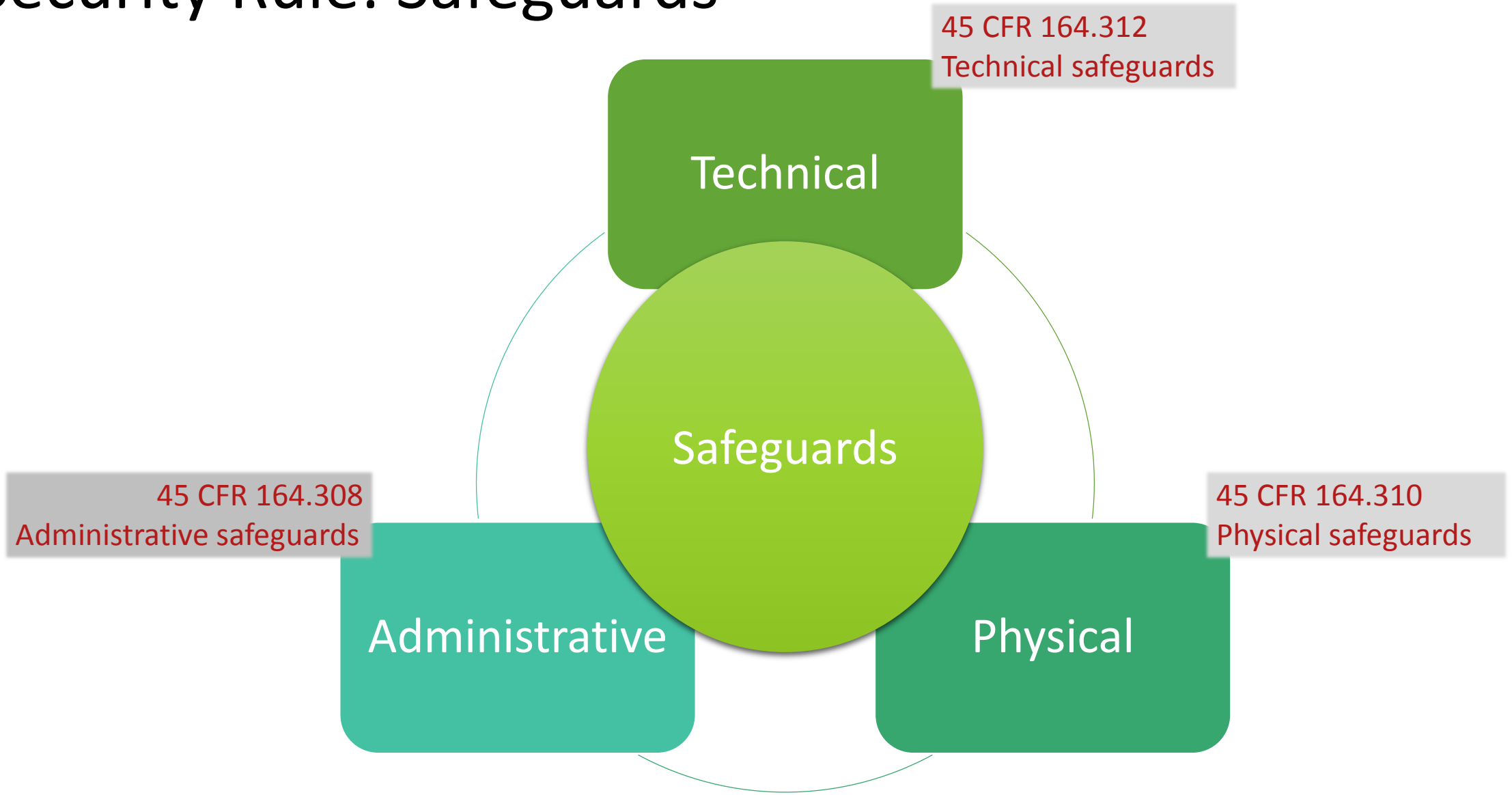
The parameters of the security risk analysis are defined 45 CFR 164.308(a)(1).

HHS Office for Civil Rights (OCR) has issued guidance on conducting a security risk analysis.

Additional tools and resources available by ONC and OCR

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Security Rule: Safeguards



Administrative Safeguards

Focus on internal organization, policies, procedures, & maintenance of security measures

- Identify and analyze risks to e-PHI (Risk Assessment)
- Training
- Information access management
- Business Continuity and Disaster Recovery

45 CFR 164.308
Administrative safeguards

High-Level Steps in Performing a Risk Analysis

1. Identify your PHI; where it is and what it's on
2. Determine costs associated with your PHI
3. Identify the threats and vulnerabilities
4. Calculate the specific risks
5. Analyze your results
6. Complete a cost-benefit analysis
7. Brief management on risks
8. Develop your risk mitigation plan

1. Identify your PHI; where it is and what it's on

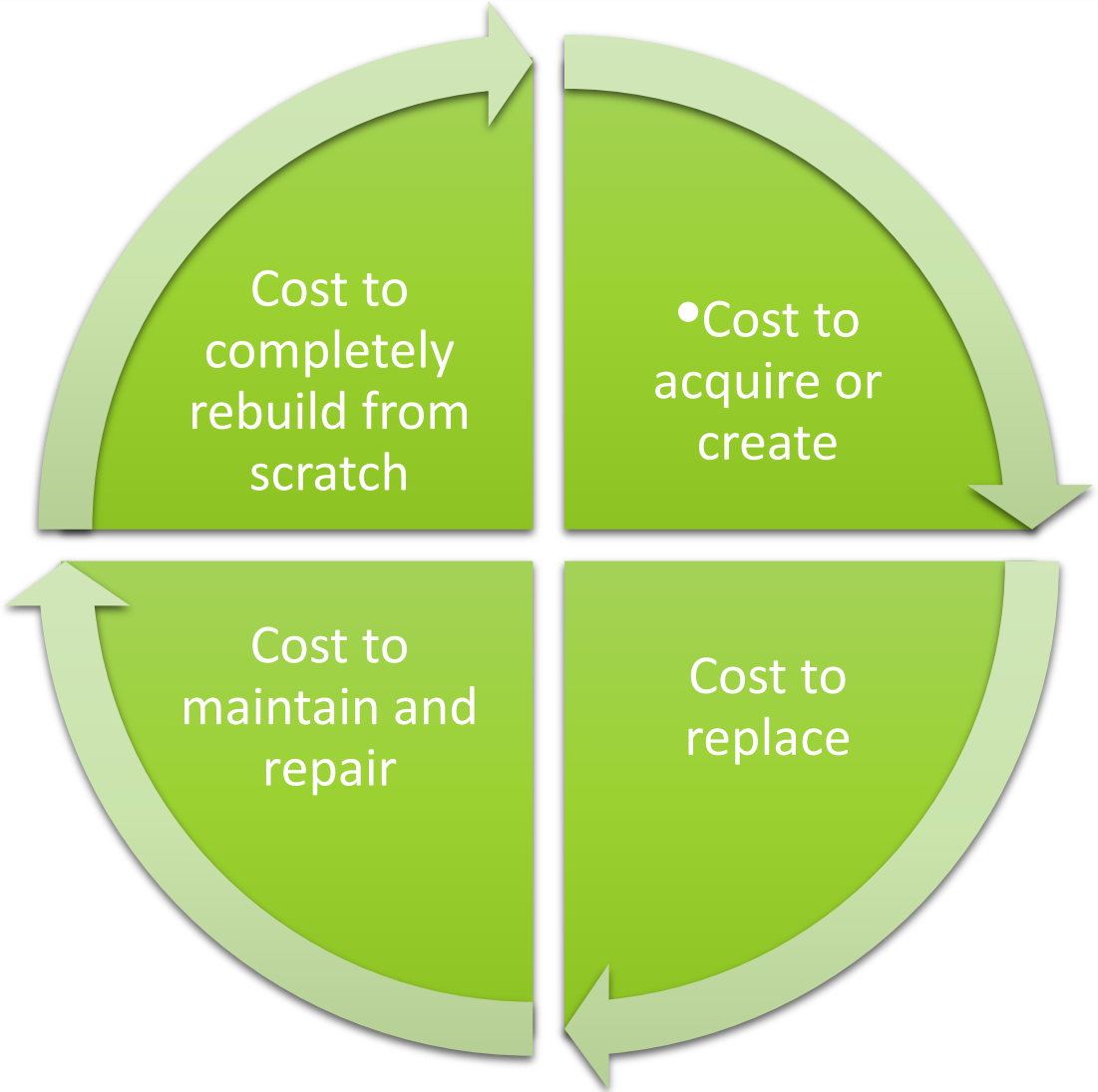
- What PHI and associated systems is your organization dependent upon?
  - Interview key personnel
  - Inventory all hardware, software, and information
  - Document information flows

Review existing policies and procedures

Review your existing technology

Prioritize findings based on criticality to the business

2. Determine costs associated with your PHI



3. Identify the threats and vulnerabilities

- Determine the specific threats and vulnerabilities associated with PHI using:
  - Automated Tools
  - Manual Assessments

Threat: An indication or intent to cause disturbance or harm to PHI

Vulnerability: An information system weakness that can be exploited or harm PHI

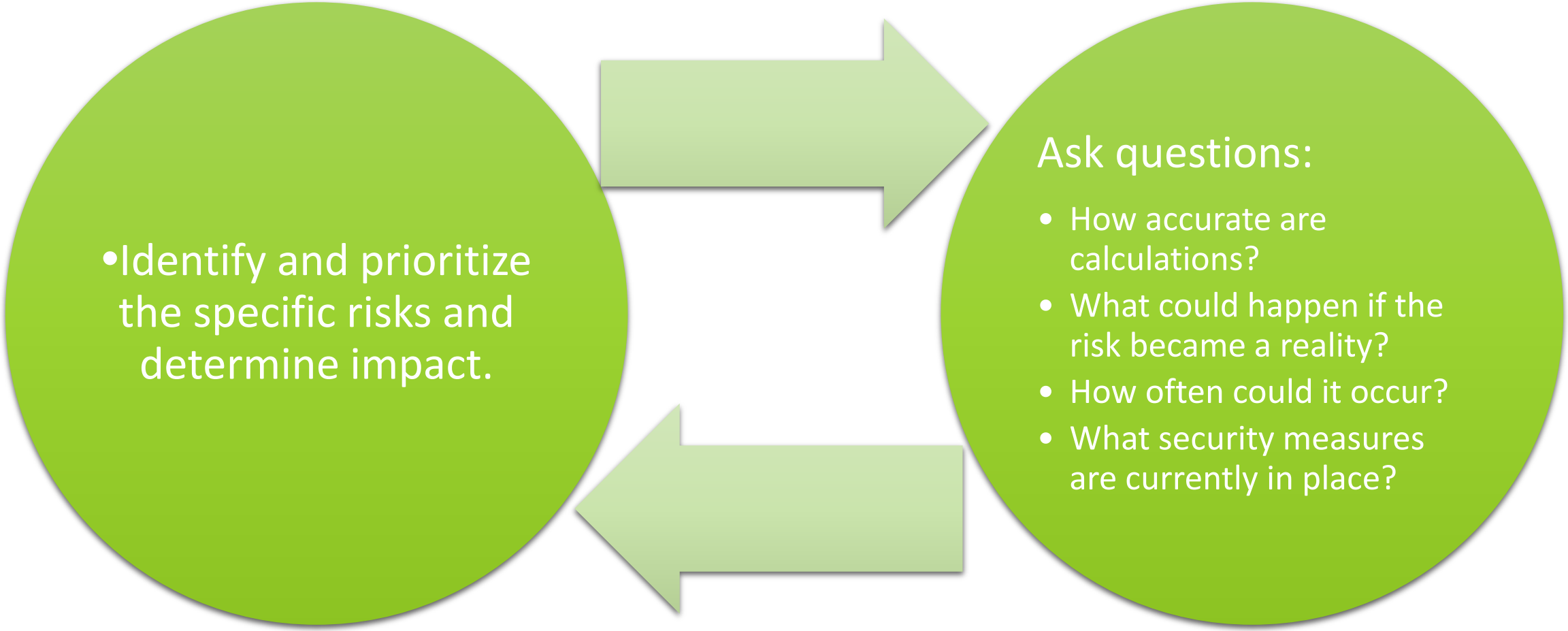
THREATS	VULNERABILITIES
Malware	OS, databases, and application with default passwords
Social engineering and phishing	No data backup system
Hackers	Using and/or posting to social media sites
Disgruntled or malicious employees	Mobile devices and wireless access
Untrained users	Security exposures due to lack of procedures or technologies
Malicious contractors	No full disk encryption on laptops
Fires, earthquakes, tornadoes, floods, etc.	SQL injection on web applications

4. Calculate the specific risks

Threat	**Vulnerability**	**Cost**
Indication of intent to inflict harm or damage	Weaknesses that can be exploited by a threat	Total economic impact of a successful attack

Risk = Threat x Vulnerability x Cost

5. Analyze your results



6. Complete a cost-benefit analysis

Determine how willing your organization is to accept those risks

Decide whether the PHI is as valuable as the cost, time, and effort it would take to protect it.

8. Determine your risk mitigation plan

Accept the risks
Get it in writing!

Reduce your risks through policies, procedures, and technologies

Transfer your risks to another entity

Physical Safeguards

Control physical access to your office and computer systems

- Facility access controls
- Workstation security measures
- Workstation use policies

45 CFR 164.310
Physical safeguards

Technical Safeguards

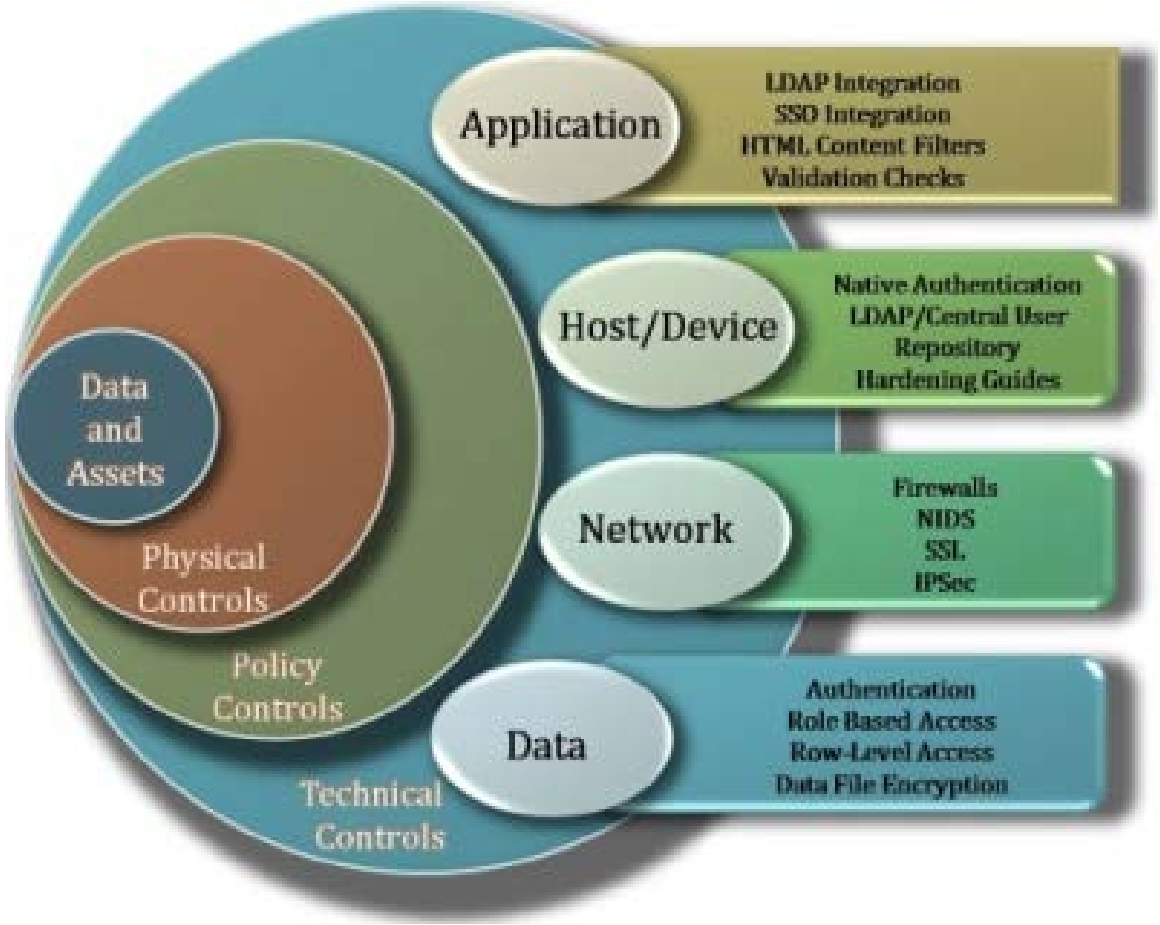


Image from esri, http://goo.gl/6WW7az

- Restrict access to ePHI
- Audit controls to monitor activity on systems containing ePHI
- Integrity controls to prevent improper ePHI alteration or destruction
- Transmission security measures to protect ePHI when transmitted over an electronic network

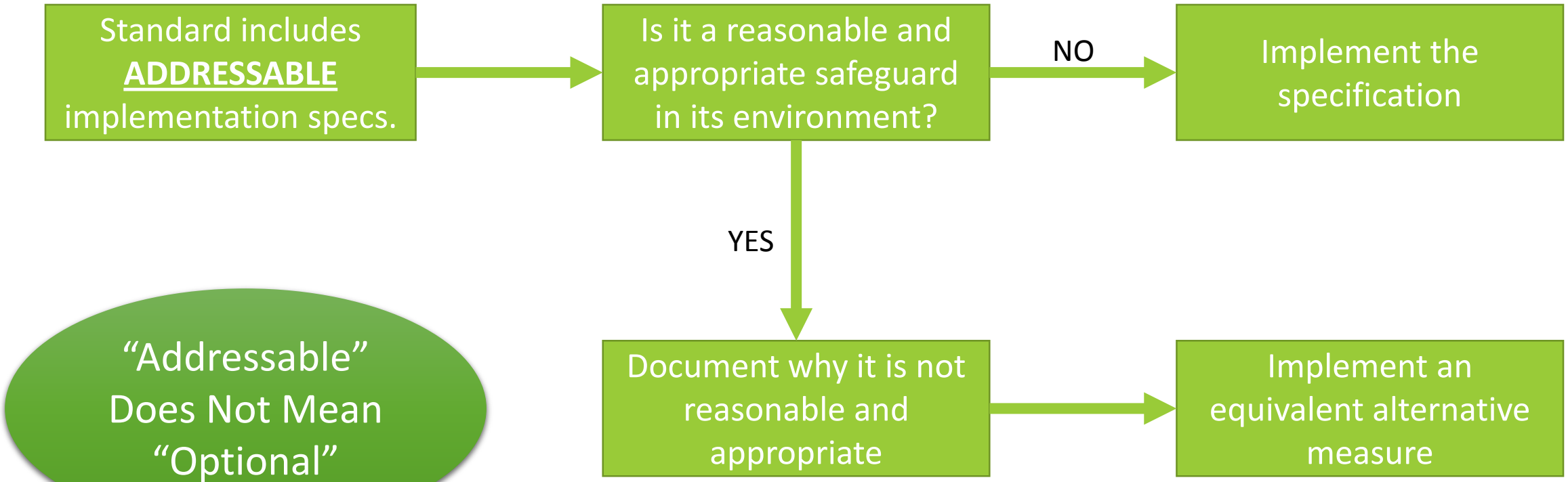
45 CFR 164.312
Technical safeguards

Required vs. Addressable

REQUIRED: 164.306 (d)(2): When a standard adopted includes required implementation specifications, a CE or BA must implement the specifications

45 CFR 164.306 - Security standards: General rules.

Required vs. Addressable



"Addressable" Does Not Mean "Optional"

Security Assessment Tools

NIST

HIPAA Security Toolkit

HHS + ONC

Security Risk Assessment Tool

HIPAA COW

Risk Assessment Tools

NIST HIPAA Security Rule Toolkit

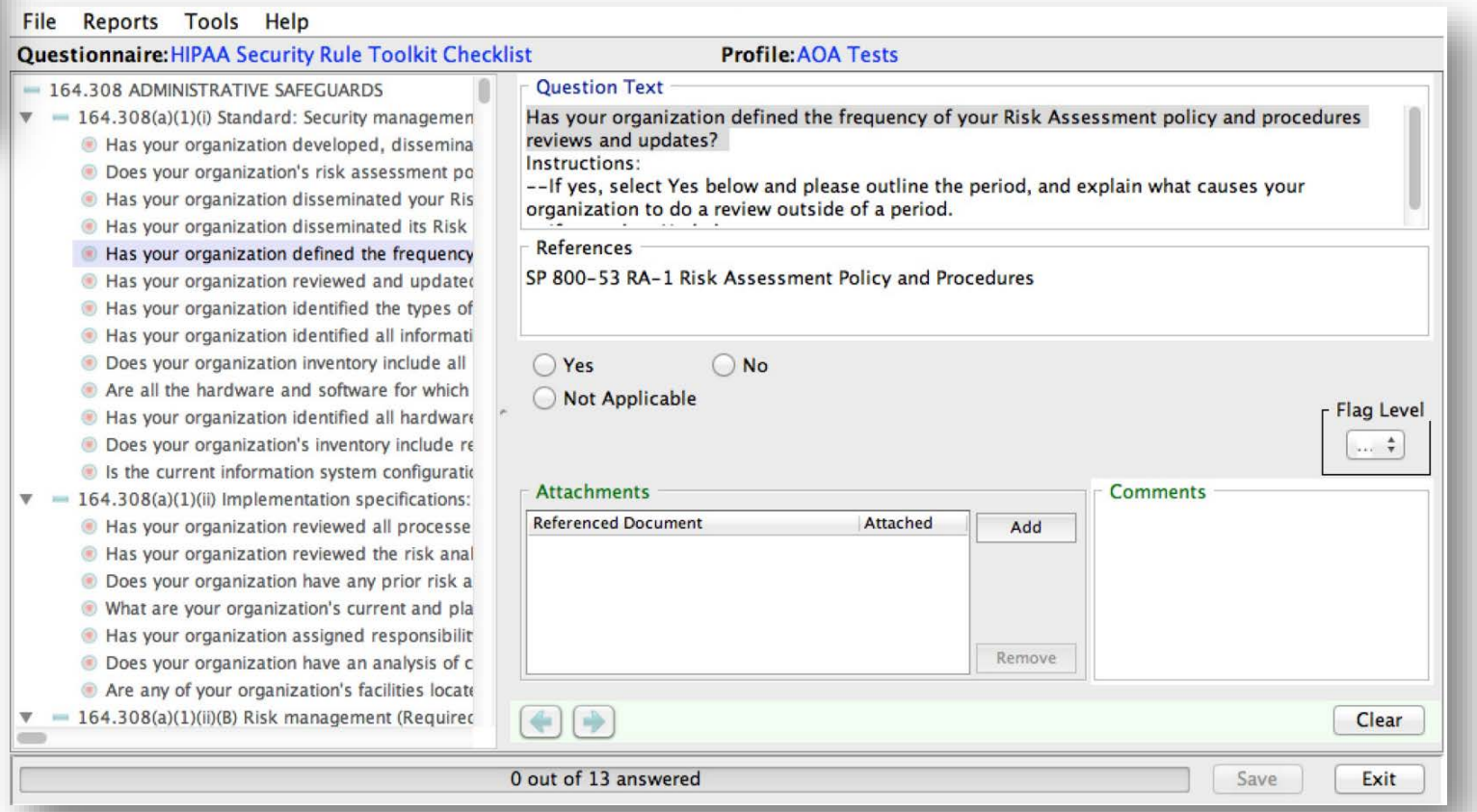
HSR Toolkit addresses implementation specifications identified in the HIPAA Security Rule.

National Institute of Standards and Technology
Information Technology Laboratory

Security Content Automation Protocol

SCAP

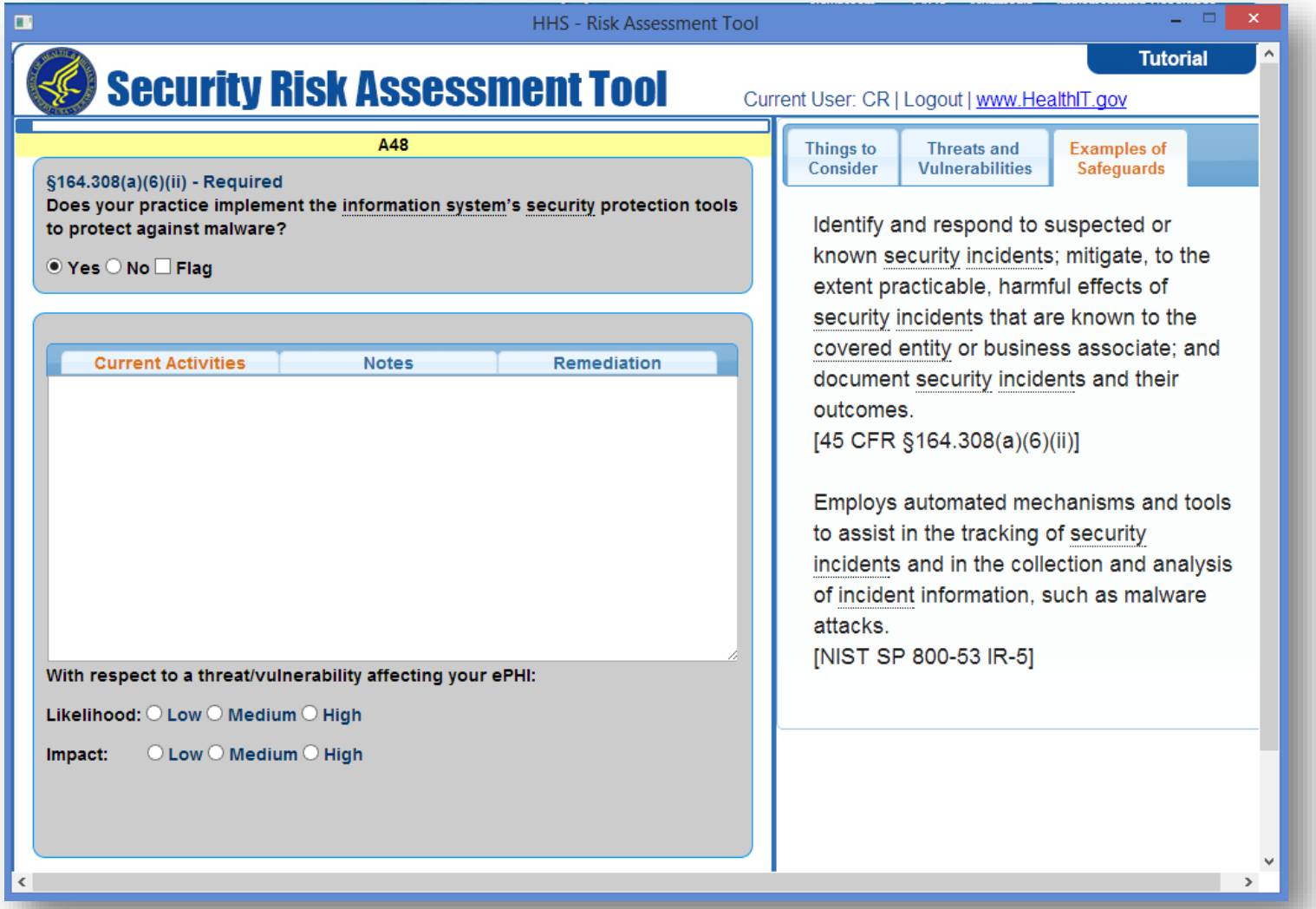
- HIPAA Security Rule
- NIST Special Publication 800-66
- NIST Special Publication 800-53
- NIST Special Publication 800-53A
- Health Information Technology for Economic and Clinical Health (HITECH) Act



https://scap.nist.gov/hipaa/

HHS/ONC Security Risk Assessment Tool

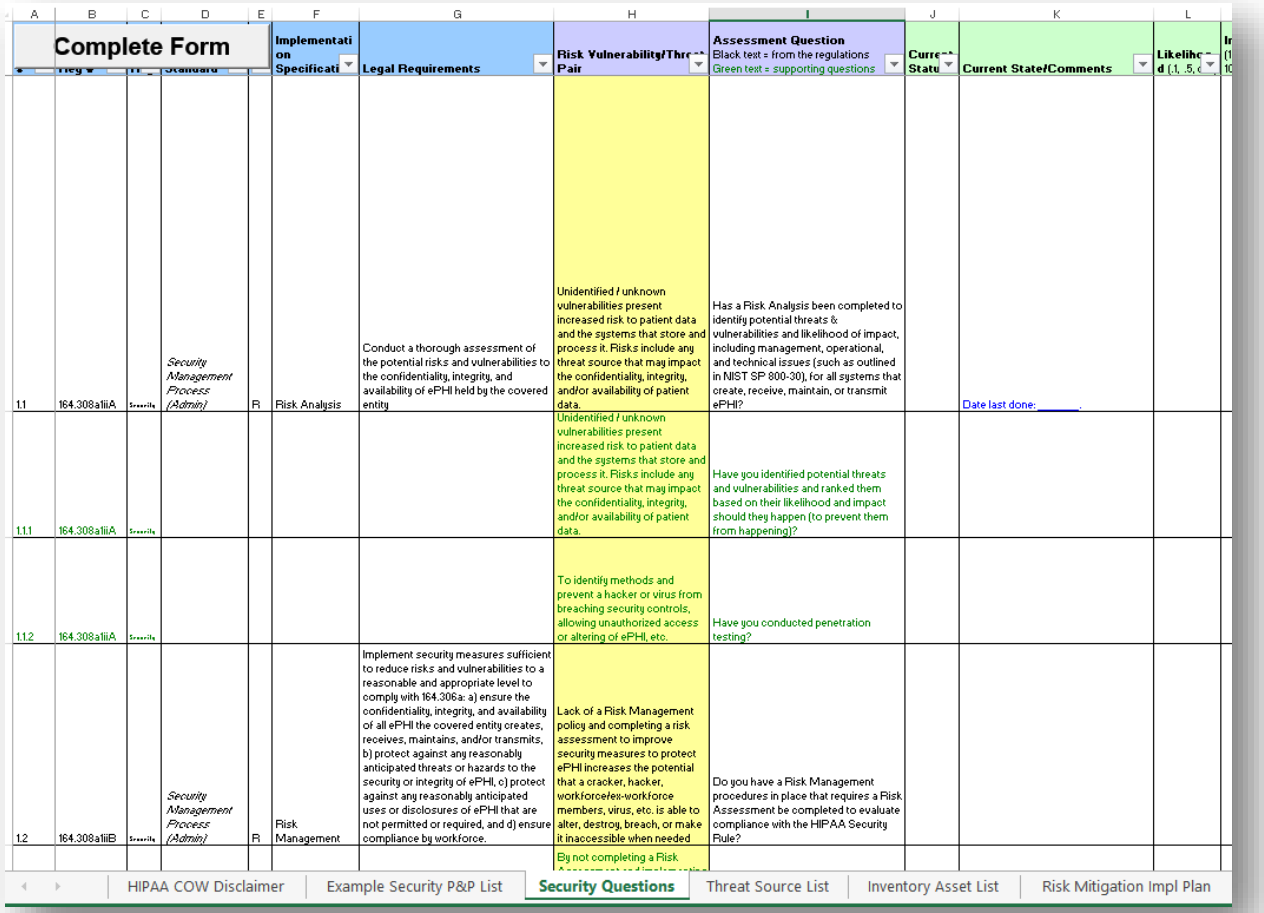
- HIPAA Security Rule
- NIST Special Publication 800-66
- NIST Special Publication 800-53
- NIST Special Publication 800-53A
- Health Information Technology for Economic and Clinical Health (HITECH) Act



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

HIPAA Collaborative of Wisconsin

1. Toolkit Guide
2. NIST Risk Assessment Steps
3. HIPAA COW Assessment Template
4. NIST Threat Overview
5. Network Diagram Examples
6. NIST Risk Definitions & Calculations
7. NIST Risk Mitigation Activities
8. HIPAA Cow Risk Analysis Report Template
9. Risk Management Policy
10. HIPAA COW OCR Audit Protocol



Complete Form					Implementation Specificati	Legal Requirements	Risk Vulnerability/Threat Pair	Assessment Question Black text = from the regulations Green text = supporting questions	Current Statu	Current State/Comments	Likelihood (.1, .5,
1.1	164.308a1iiA	Security	*Security Management Process (Admin)*	R	Risk Analysis	Conduct a thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity	Unidentified / unknown vulnerabilities present increased risk to patient data and the systems that store and process it. Risks include any threat source that may impact the confidentiality, integrity, and/or availability of patient data.	Has a Risk Analysis been completed to identify potential threats & vulnerabilities and likelihood of impact, including management, operational, and technical issues (such as outlined in NIST SP 800-30), for all systems that create, receive, maintain, or transmit ePHI?		Date last done:_____.	
1.1.1	164.308a1iiA	Security					Unidentified / unknown vulnerabilities present increased risk to patient data and the systems that store and process it. Risks include any threat source that may impact the confidentiality, integrity, and/or availability of patient data.	Have you identified potential threats and vulnerabilities and ranked them based on their likelihood and impact should they happen (to prevent them from happening)?			
1.1.2	164.308a1iiA	Security					To identify methods and prevent a hacker or virus from breaching security controls, allowing unauthorized access or altering of ePHI, etc.	Have you conducted penetration testing?			
1.2	164.308a1iiB	Security	*Security Management Process (Admin)*	R	Risk Management	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306a: a) ensure the confidentiality, integrity, and availability of all ePHI the covered entity creates, receives, maintains, and/or transmits, b) protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, c) protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required, and d) ensure compliance by workforce.	Lack of a Risk Management policy and completing a risk assessment to improve security measures to protect ePHI increases the potential that a cracker, hacker, workforce/ex-workforce members, virus, etc. is able to alter, destroy, breach, or make it inaccessible when needed	Do you have a Risk Management procedures in place that requires a Risk Assessment be completed to evaluate compliance with the HIPAA Security Rule?			
							By not completing a Risk				

HIPAA COW Disclaimer | Example Security P&P List | **Security Questions** | Threat Source List | Inventory Asset List | Risk Mitigation Impl Plan

CELEBRATING 15 YEARS
2001-2016

hipaacow.org fm

http://hipaacow.org/resources/hipaa-cow-documents/risk-toolkit/

HIPAA COW is a non-member 501(c)(3) corporation, a not-for-profit charitable organization.

Performing Ongoing HIPAA Compliance Reviews & Audits

Audit Validation: Security risk analysis of the certified EHR technology was performed prior to the date of attestation on an annual basis and for the certified EHR technology used during the EHR reporting period.

INFORMATION NEEDED FOR AUDIT

- ✓ Privacy policies and procedures
- ✓ Security policies and procedures
- ✓ All forms of PHI stored or transmitted both in hard copy and electronic formats
- ✓ The methods and systems in place to protect PHI

PRACTICAL CHECKLIST

- ✓ Is someone in charge of HIPPA privacy and security compliance?
- ✓ Are privacy and security audits being performed annually?
- ✓ Are policies and procedures being updated and added as needed?
- ✓ Does regular information security and privacy training occur?
- ✓ Are you documenting your ongoing HIPAA audits?
- ✓ Are you integrating privacy and security compliance into the overall risk management program?

Documentation to support attestation data should be retained for six years post-attestation.

10 Myths of Security Risk Analysis

1. The security risk analysis is optional for small providers.

False. All providers who are “covered entities” under HIPAA are required to perform a risk analysis.

2. Simply installing a certified EHR fulfills the security risk analysis MU requirement.

False. Even with a certified EHR, you must perform a full security risk analysis.

3. My EHR vendor took care of everything I need to do about privacy and security.

False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules.

4. I have to outsource the security risk analysis.

False. It is possible for small practices to do risk analysis themselves using self-help tools.

5. A checklist will suffice for the risk analysis requirement.

False. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.

10 Myths of Security Risk Analysis cont'd

6. There is a specific risk analysis method that I must follow.

False. A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule.

7. My security risk analysis only needs to look at my EHR.

False. Review all electronic devices that store, capture, or modify electronic protected health information.

8. I only need to do a risk analysis once.

False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections.

9. Before I attest for an EHR incentive program, I must fully mitigate all risks.

False. The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) during the reporting period, as part of its risk management process.

10. Each year, I'll have to completely redo my security risk analysis.

False. Under the Meaningful Use Programs, reviews are required for each EHR reporting period. For EPs, the EHR reporting period will be 90 days or a full calendar year, depending on the EP's year of participation in the program.

Resources

- https://scap.nist.gov/hipaa/
- http://hipaacow.org/resources/hipaa-cow-documents/risk-toolkit/
- https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/2015EP_1ProtectPatientHealthInfoObjective.pdf
- Rebecca Herold and Kevin Beaver, “The Practical Guide to HIPAA Privacy and Security Compliance” 2nd Edition, 2015