HOLLAND&HART LLP™

HIPAA Security Rule: Annual Checkup

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.

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 improvement 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/
http://www.healthcareitnews.com/news/ohsu-pays-27-million-fine-hhs-office-civil-rights-two-hipaa-breaches

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

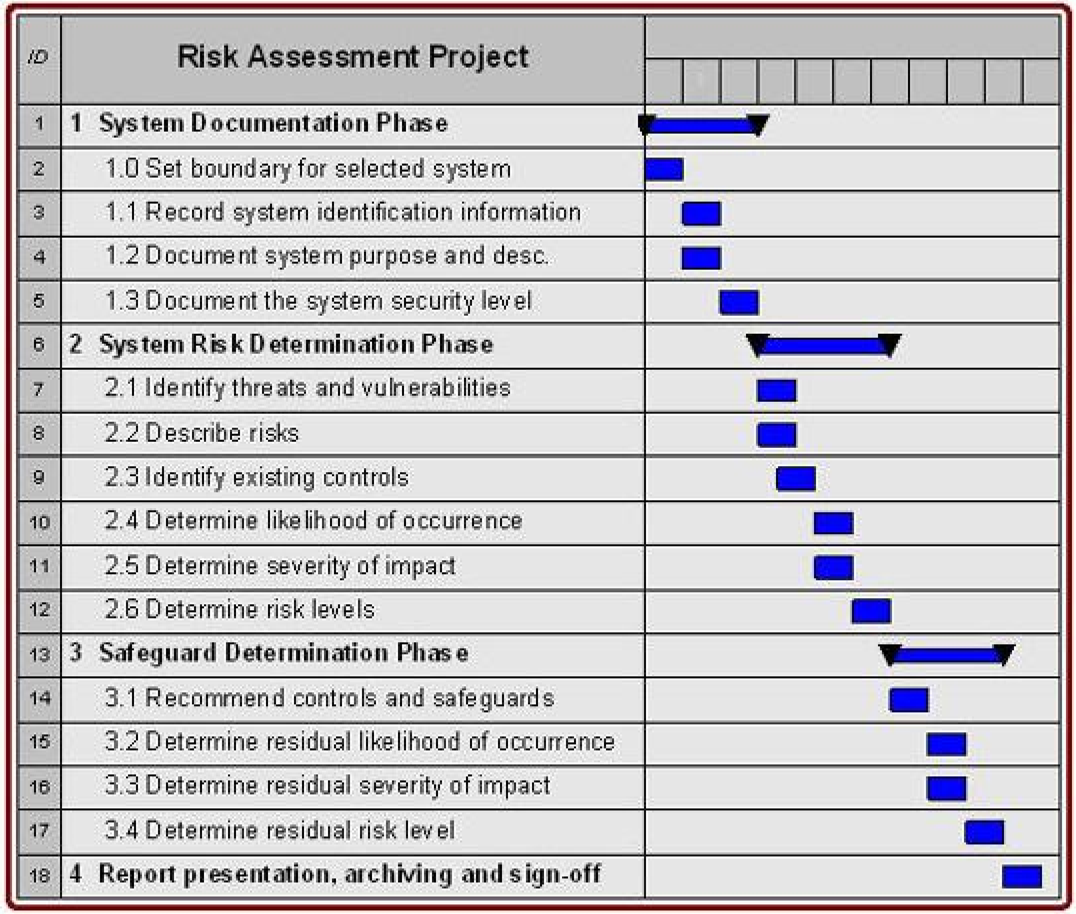
- **45 CFR 164.302-318**
- **164.306 (General Requirements)**
  - (a)(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
  - (a)(2) Protect against any reasonably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

- 164.308 (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).

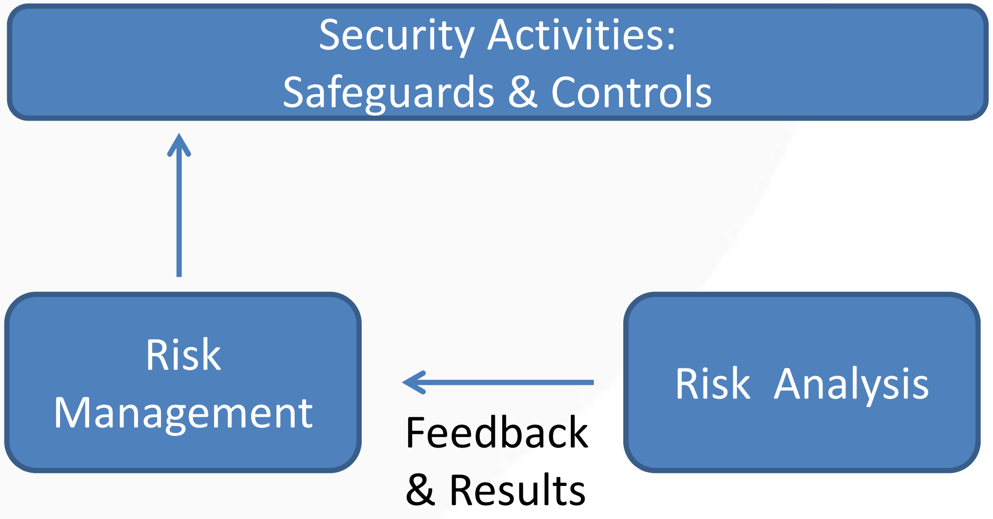
HIPAA Security Rule - Documentation

- 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



Security Activities:
Safeguards & Controls

Risk Management

Feedback & Results

Risk Analysis

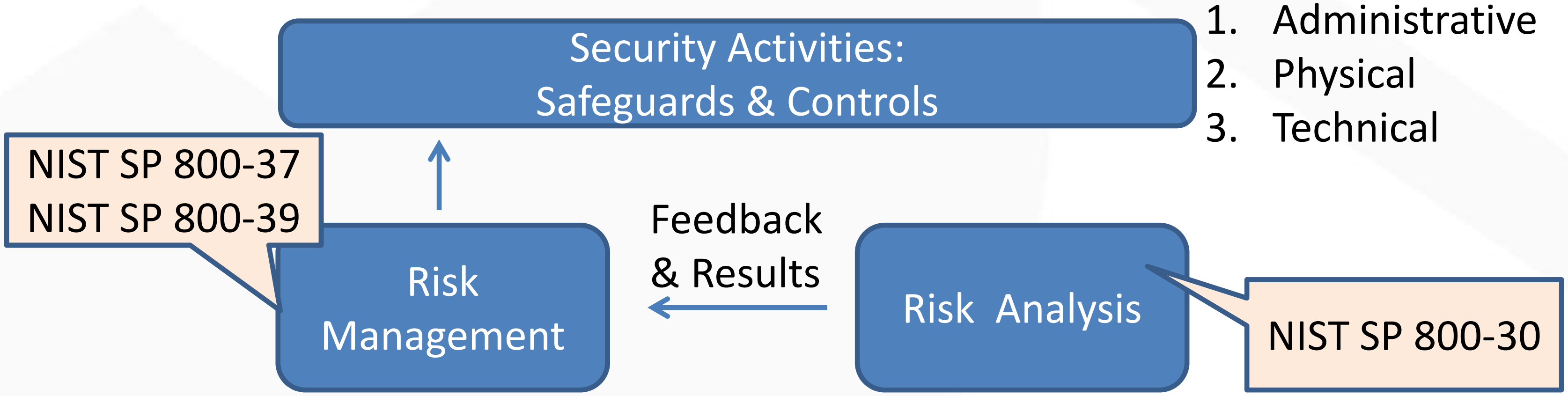
NIST Standards

"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

Risk Management & Analysis



Security Activities:
Safeguards & Controls

1. Administrative
2. Physical
3. Technical

NIST SP 800-37
NIST SP 800-39

Risk Management

Feedback
& Results

Risk Analysis

NIST SP 800-30

1. Develop and implement a risk management plan.
2. Implement security measures.
3. Evaluate and maintain security measures.

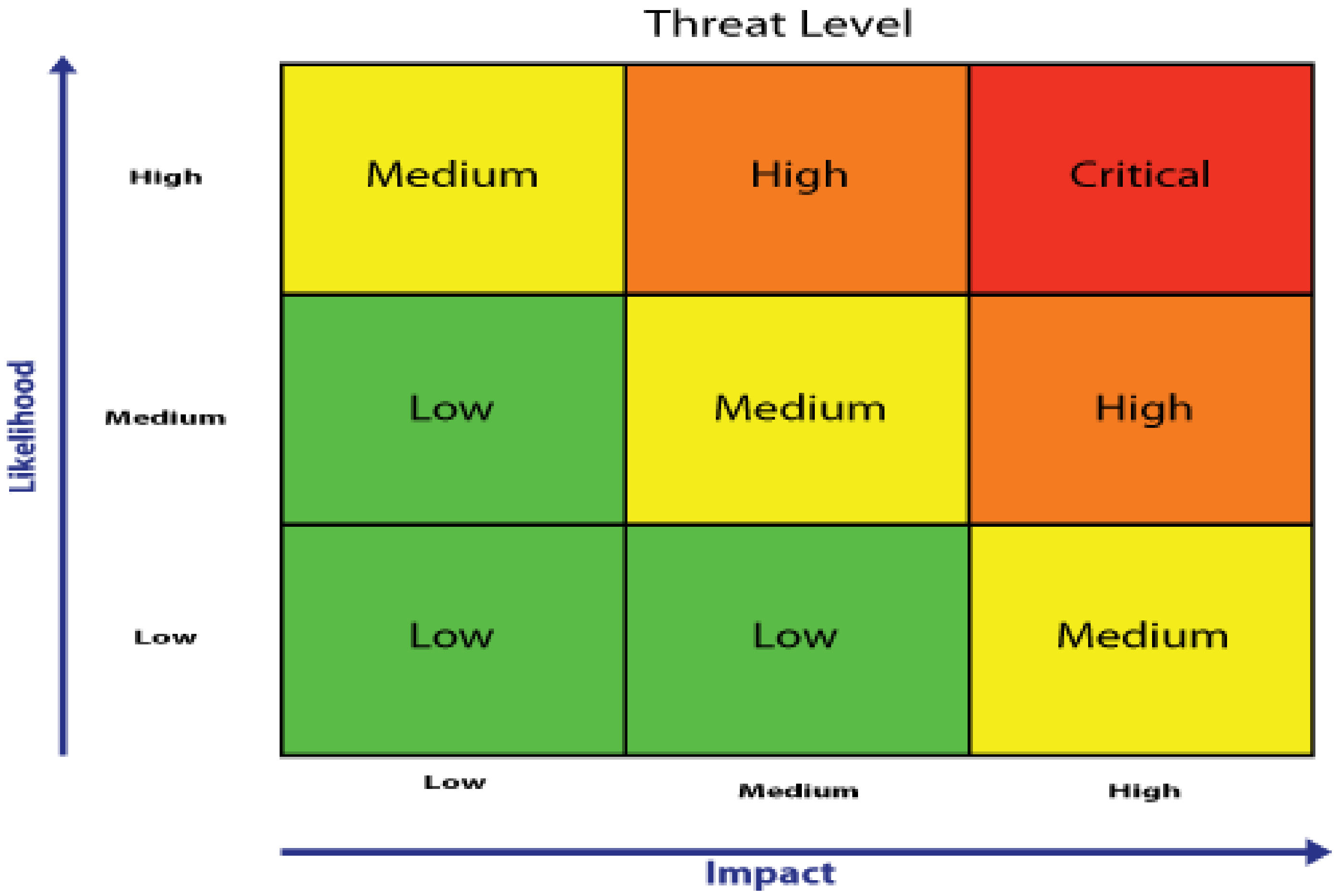
1. Identify the scope of the analysis.
2. Gather data.
3. Identify and document potential threats and vulnerabilities.
4. Assess current security measures.
5. Determine the likelihood of threat occurrence.
6. Determine the potential impact of threat occurrence.
7. Determine the level of risk.
8. Identify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



Threat Level

Likelihood

	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

Impact

Source: http://the-outsourcing.com/subpage.php?pn=region&regid=1&aid=274

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

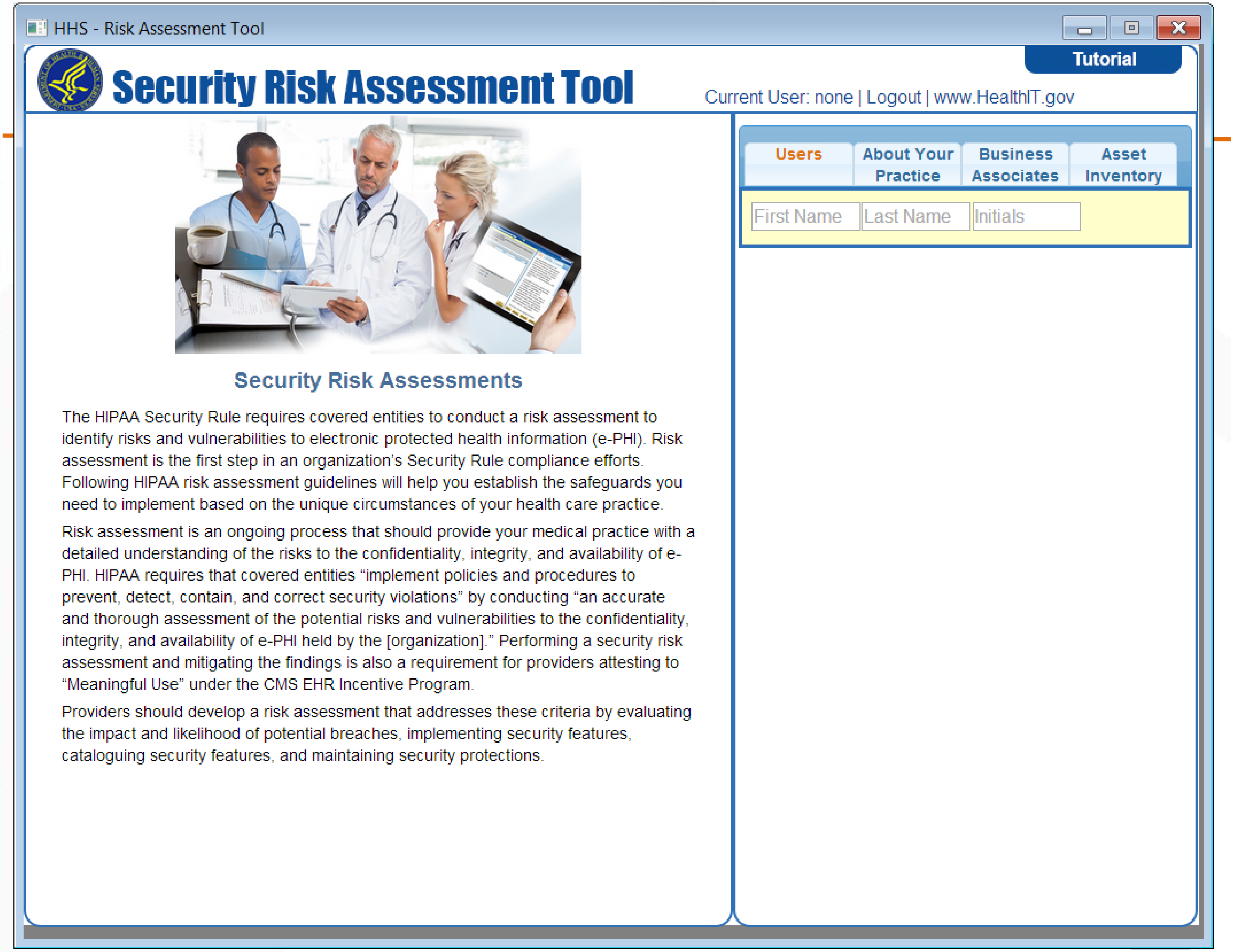
Risk Assessment

- 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 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

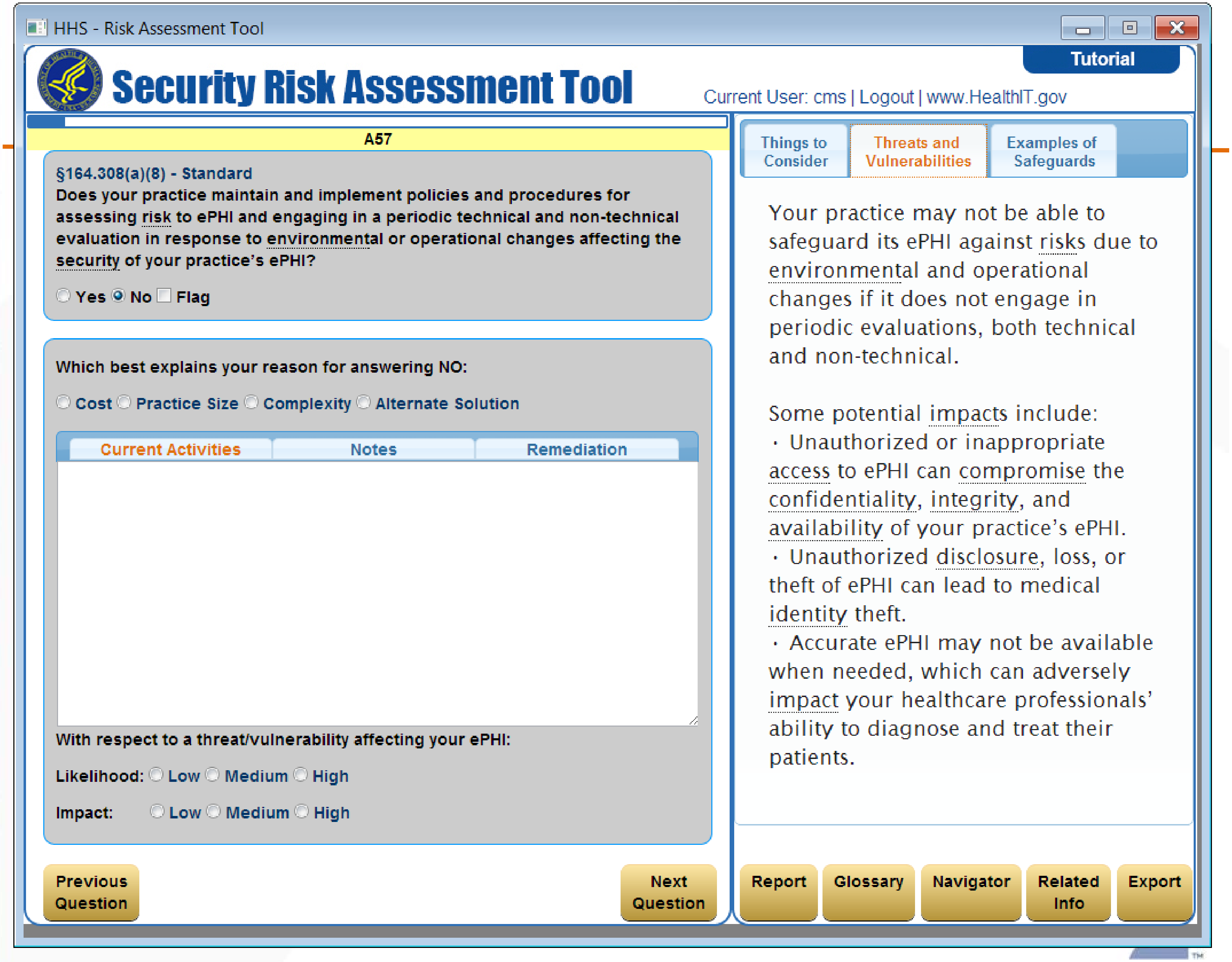

HHS - Risk Assessment Tool
Tutorial
Security Risk Assessment Tool
Current User: none | Logout | www.HealthIT.gov
Users
About Your Practice
Business Associates
Asset Inventory
First Name
Last Name
Initials

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.



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

With respect to a threat/vulnerability affecting your ePHI:

Likelihood: ○ Low ○ Medium ○ High

Impact: ○ Low ○ Medium ○ High

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.

Required & Addressable Safeguards

Required vs. Addressable

- Required
  - the implementation specification must be implemented
- Addressable
  - The concept of "addressable implementation specifications" was developed to provide covered entities additional flexibility with respect to compliance with the security standards.

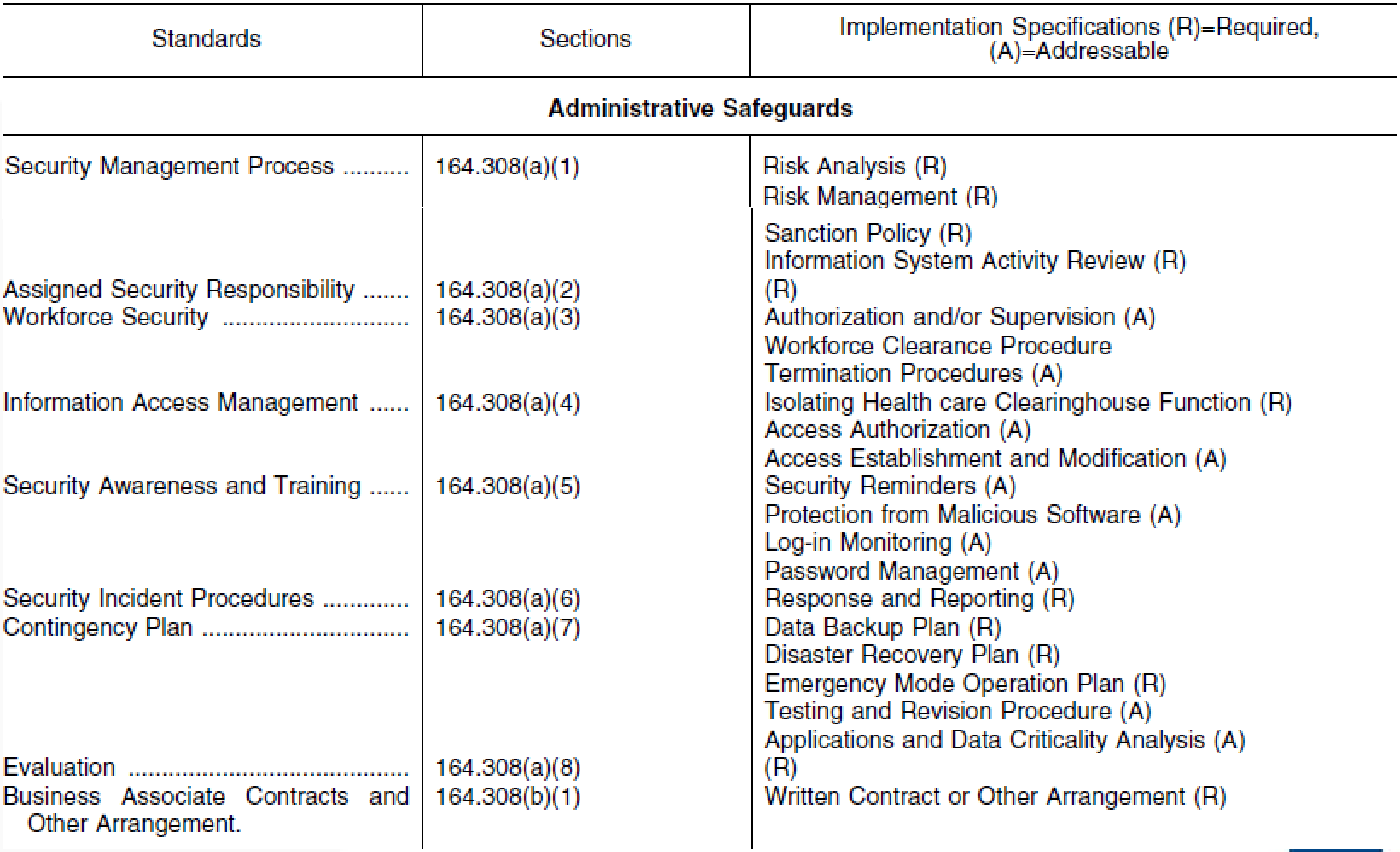
Addressable

- 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)
  - (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.)
  - (c) not implement either an addressable implementation specification or an alternative.

Documentation of Decisions

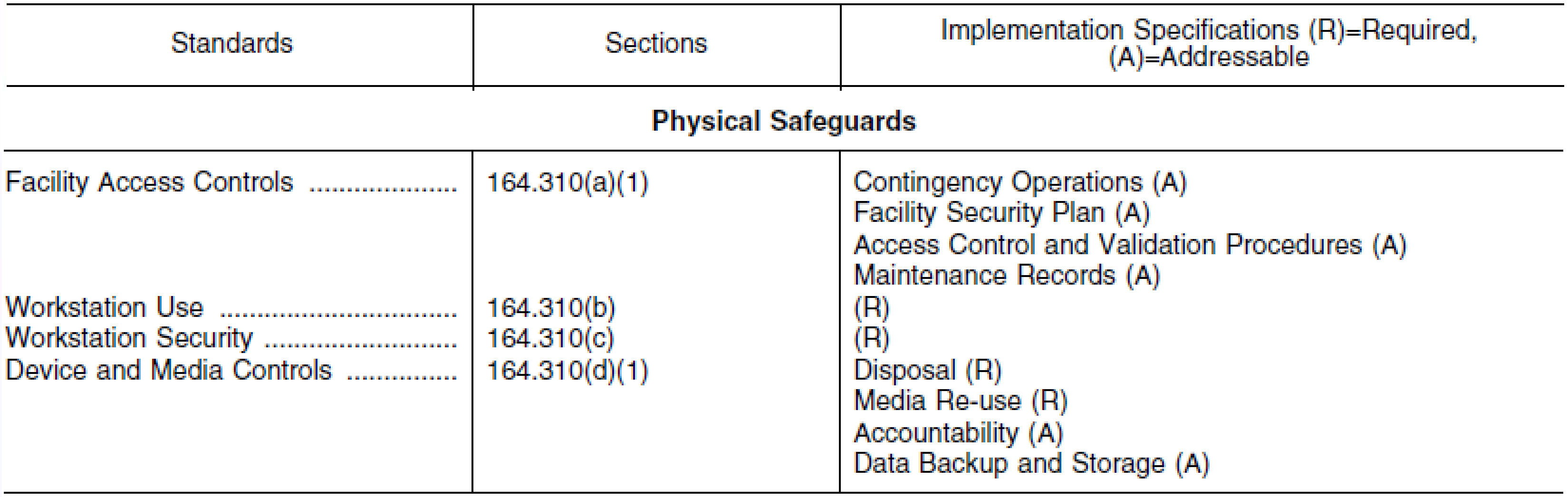
- This decision will depend on a variety of factors such as:
  - the entity's risk analysis,
  - risk mitigation strategy,
  - what security measures are already in place,
  - the cost of implementation.
- The decisions that a covered entity makes regarding addressable specifications must be documented 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.

Administrative Safeguards



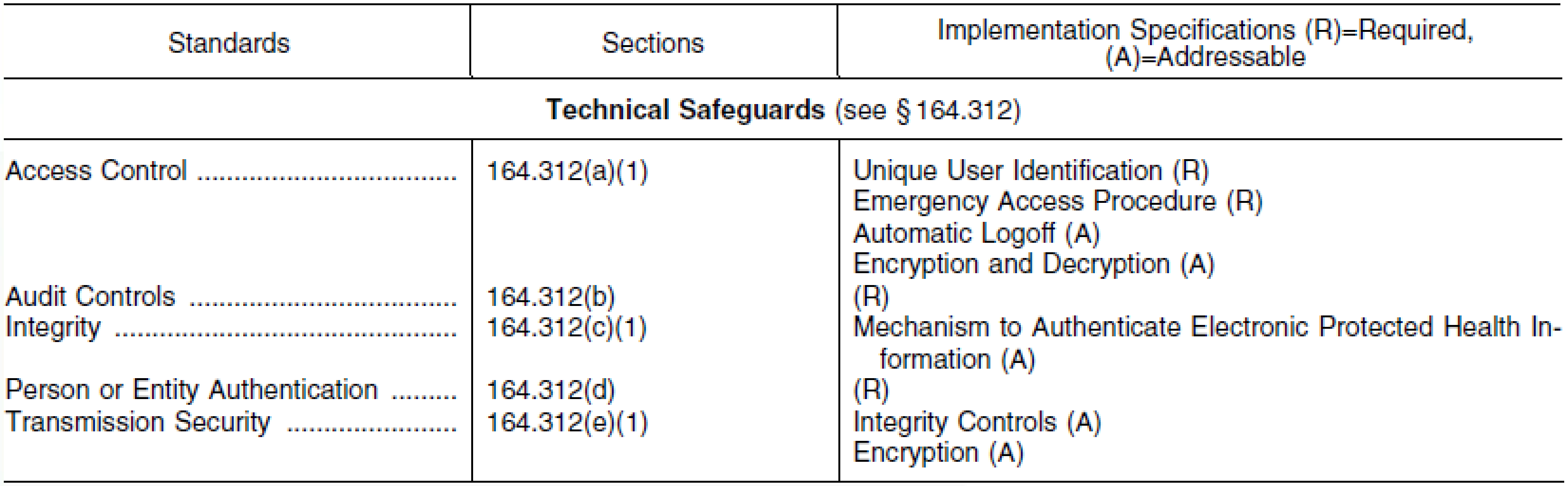
Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce 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)

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

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

Encryption

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 database
  - in flat files
- 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
https://www.healthit.gov/providers-professionals/five-steps-organizations-can-take-manage-mobile-devices-used-health-care-pro

Hot Topics

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

NIST Cybersecurity Framework

- Barack Obama, Exec Order 13636 (Feb. 2013)
  - Improving Critical Infrastructure Cybersecurity
  - Partnership between government and owners and operators of critical infrastructure
  - Improve cybersecurity information sharing
    - ISAOs & ISACs (See EO 13691)
  - Collaboratively develop and implement risk-based standards
  - NIST had one year to:
    - work with private sector
    - identify existing voluntary consensus standards and industry best practices
    - build them into a Cybersecurity Framework

PPD 21: Critical Infrastructure Security

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Govt. Facilities
- Healthcare & Public Health
- Nuclear Reactors, Materials, Waste
- Transportation
- Water and Wastewater

NIST Cybersecurity Framework

- NIST CSF (Feb. 2014)
- Goal: Using the Framework’s structure will drive companies to ask the right questions and begin to implement the right solutions for their particular company and industry

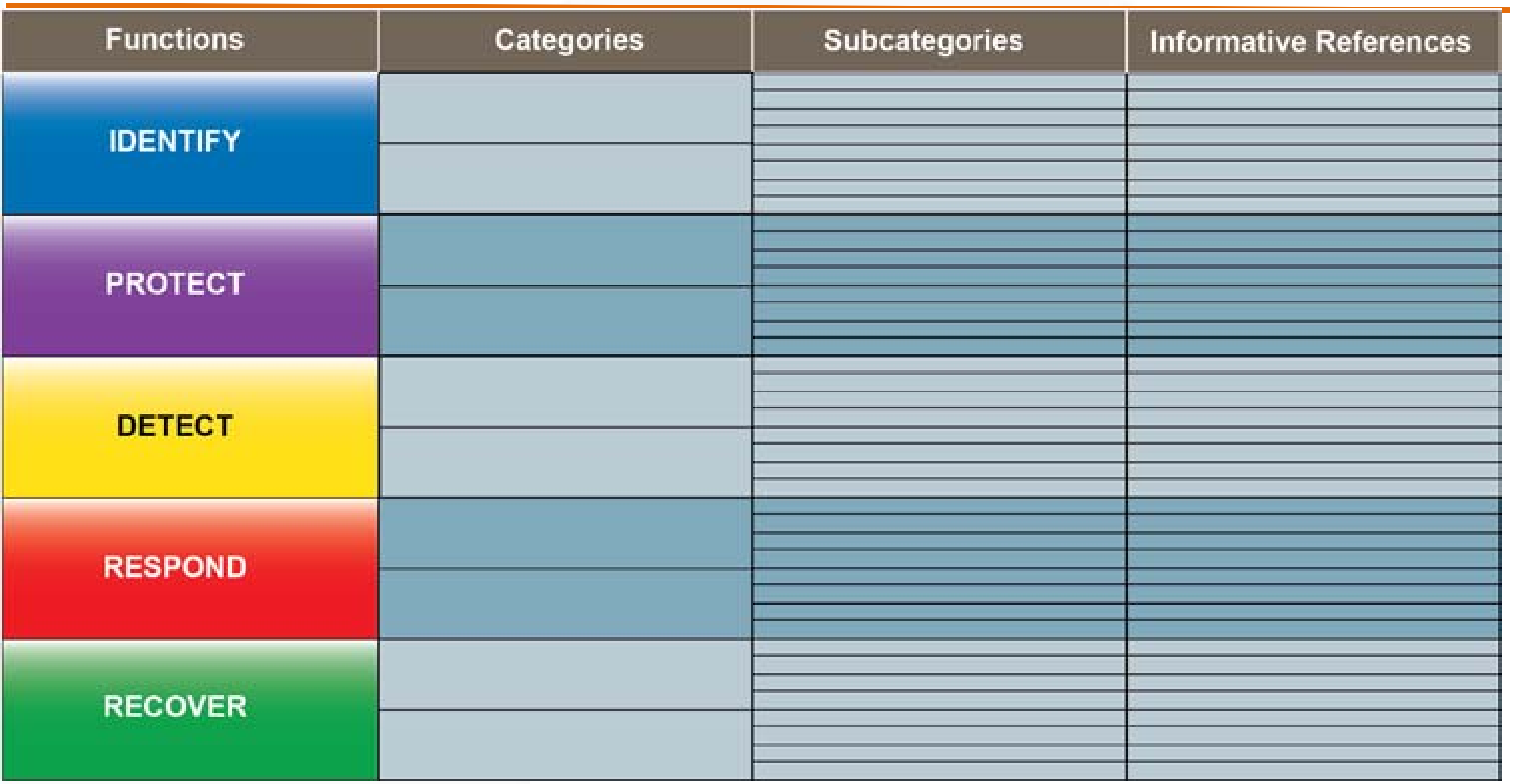
NIST CSF

- Not one-size-fits-all
- Complements, and does not replace, an organization's risk management process and cybersecurity program (assuming one exists)
- Three Parts:
  - Core
  - Profile
  - Implementation Tiers
- Contains a methodology to protect:
  - individual privacy
  - civil liberties

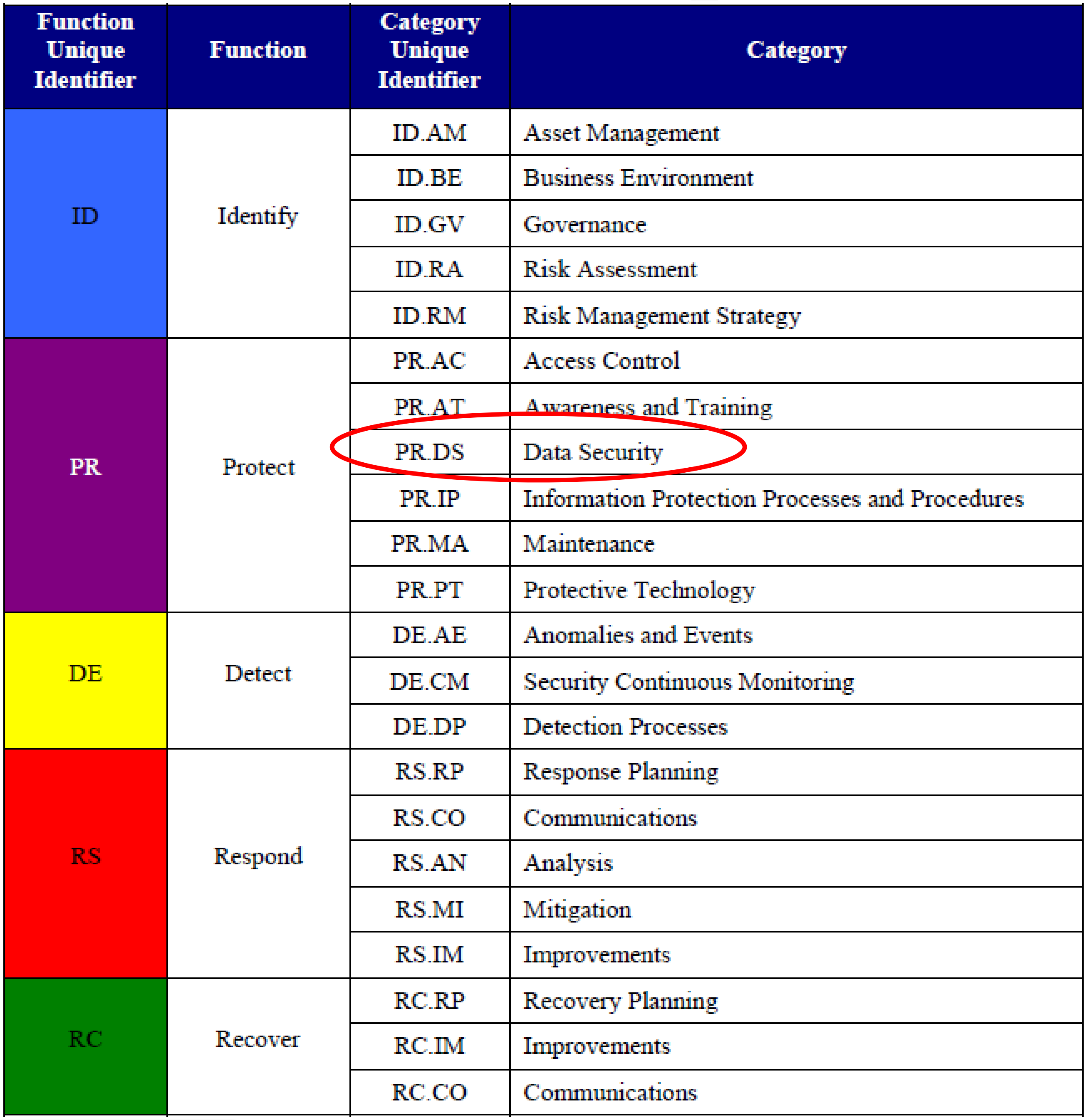
NIST CSF

- Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:
  - Describe their **current** cybersecurity **posture**;
  - Describe their **target state** for cybersecurity;
  - Identify and **prioritize** opportunities for **improvement** within the context of a continuous and repeatable process;
  - Assess **progress** toward the target state;
  - **Communicate** among internal and external stakeholders about cybersecurity risk.

NIST CSF: CORE

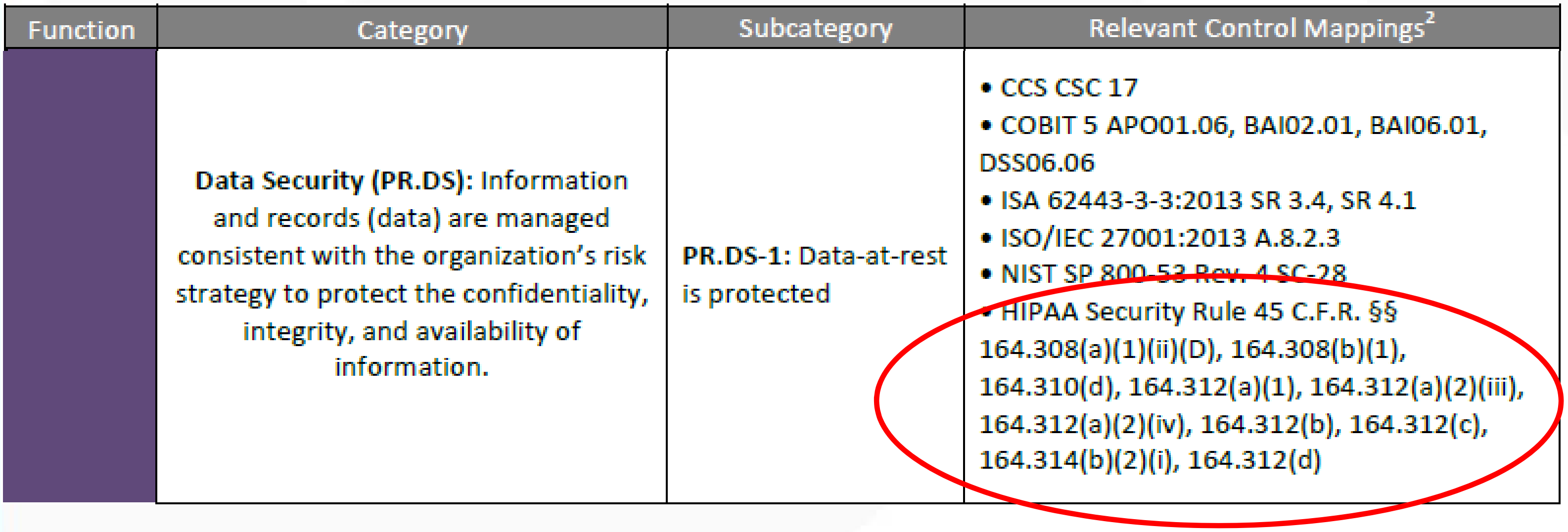


Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			



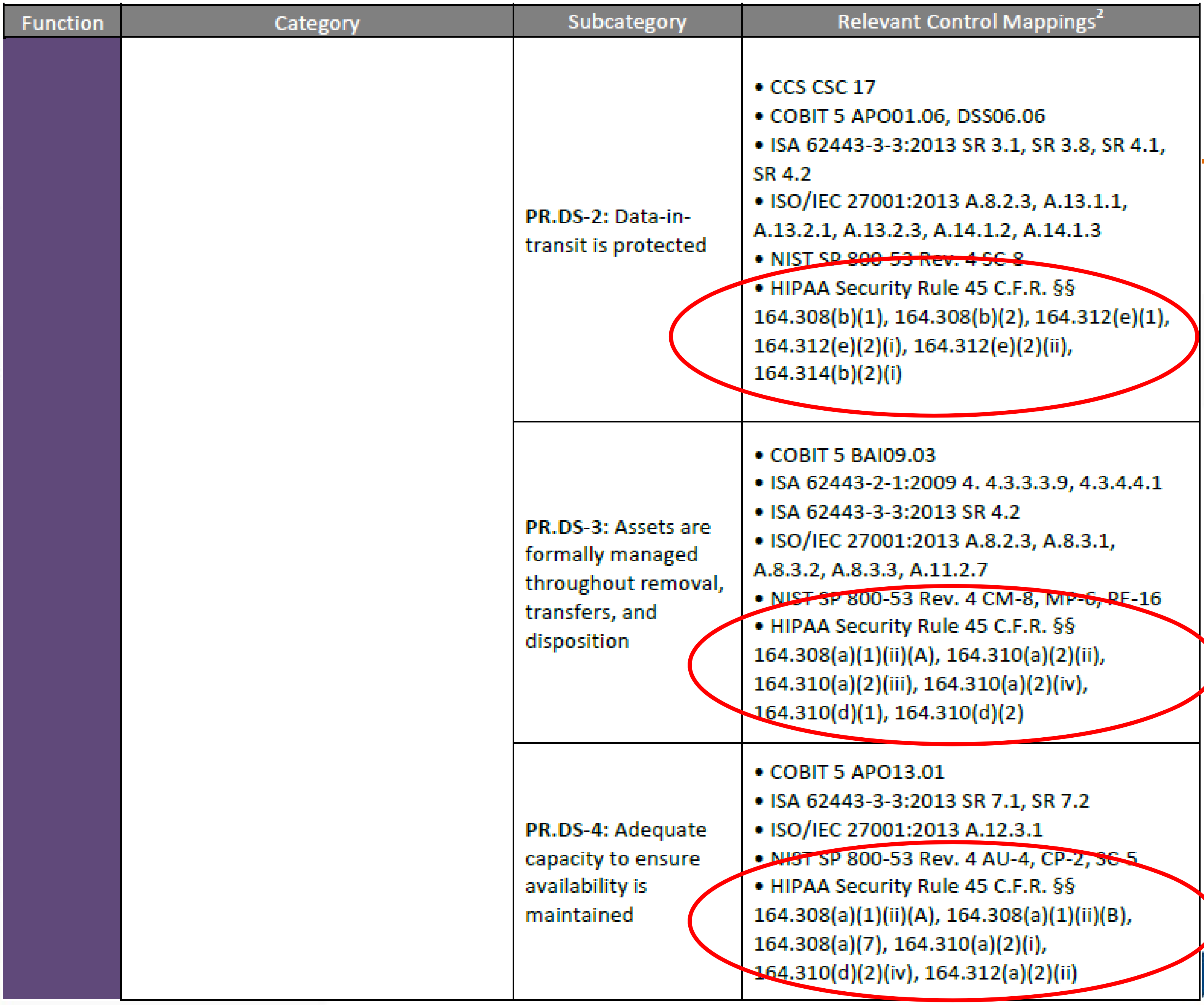
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Function	Category	Subcategory	Informative References
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	• **CCS** CSC 17 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 • **ISA 62443-3-3:2013** SR 3.4, SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3 • **NIST SP 800-53 Rev. 4** SC-28
		PR.DS-2: Data-in-transit is protected	• **CCS** CSC 17 • **COBIT 5** APO01.06, DSS06.06 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1 SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SC-8
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8. A.8.3.3, A.11.2.7 • **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-1
		PR.DS-4: Adequate capacity to ensure availability is maintained	• **COBIT 5** APO13.01 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.3.1



Function	Category	Subcategory	Relevant Control Mappings[2]
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	• CCS CSC 17 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 • ISA 62443-3-3:2013 SR 3.4, SR 4.1 • ISO/IEC 27001:2013 A.8.2.3 • NIST SP 800-53 Rev. 4 SC-28 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)

Source:
https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html?language=es



Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.DS-2: Data-in-transit is protected	• CCS CSC 17 • COBIT 5 APO01.06, DSS06.06 • ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SC-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(b)(1), 164.308(b)(2), 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii), 164.314(b)(2)(i)
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 • ISA 62443-3-3:2013 SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)
		PR.DS-4: Adequate capacity to ensure availability is maintained	• COBIT 5 APO13.01 • ISA 62443-3-3:2013 SR 7.1, SR 7.2 • ISO/IEC 27001:2013 A.12.3.1 • NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7), 164.310(a)(2)(i), 164.310(d)(2)(iv), 164.312(a)(2)(ii)

Implementation Tiers

- Factors
  - Risk Management Process
    - ad hoc, reactive, formal?
  - Integrated Risk Management Program
    - information sharing internally, executive support, funding, measurement
  - External Participation
    - ability to interact and share information externally
- Tiers
  - Partial
  - Risk Informed
  - Repeatable
  - Adaptive

How To Use NIST CSF

- Basic review of cybersecurity practices
  - Functions, categories, subcategories
- Communicate cybersecurity requirements with stakeholders
- Identify opportunities for new or revised informative references

How To Use NIST CSF (cont.)

- Establish or Improve A Cybersecurity Program
  - Step 1: Prioritize and Scope
  - Step 2: Orient
    - systems, information, assets, regulatory
  - Step 3: Create a Current Profile
    - which categories/subcategories are working
  - Step 4: Conduct a Risk Assessment
    - discern likelihood and impact (more next time)
    - incorporate threat and vulnerability information
  - Step 5: Create a Target Profile
    - which categories/subcategories are needed
  - Step 6: Determine, Analyze, Prioritize Gaps
    - Compare current to target profile
  - Step 7: Implement Action Plan

HOLLAND&HART

Thanks for Participating

Kim Stanger
kcstanger@hollandhart.com

Matt Sorensen
cmsorensen@hollandhart.com