HIPAA Security 101

Catherine M. Boerner, JD, CHC
Boerner Consulting LLC

Today's Webinar is Sponsored by:

AxCel Technology

Hello Phoenix

von Briesen
von Briesen & Roper, s.c. | Attorneys at Law

hipaacow.org®

Date Recorded:
September 26, 2019

HIPAA COW Mission

- Assist HIPAA Covered Entities, Business Associates, and other interested parties in implementing HIPAA's Privacy, Security and EDI Standard Transaction provisions, as amended over time.
- Foster public education about HIPAA.
- Facilitate and streamline HIPAA implementation through identification of best practices.
- Reduce duplicate efforts among entities obligated to comply with HIPAA.
- Offer opportunities for partnering and collaborating between entities implementing HIPAA.
- Identify and evaluate new or difficult HIPAA interpretation issues.

Disclaimer

HIPAA Collaborative of Wisconsin (“HIPAA COW”) holds the Copyright © to this Security 101 Webinar (“Document”). HIPAA COW retains full copyright ownership, rights and protection in all material contained in this Document. Any HIPAA COW copyrighted document may be downloaded from the web, printed, and distributed in its entirety as long as: (i) the reproduced document contains the original HIPAA COW copyright and disclaimer and (ii) the document is provided free of charge. Any entity who wishes to adopt part or all of a document for its own internal compliance may do so without the copyright as long as the document is adopted solely for internal purposes and HIPAA COW is referenced as a source. Any other use of copyrighted material is prohibited without the express written permission of HIPAA COW. This Document is provided “as is” without any express or implied warranty. This Document is for educational purposes only and does not constitute legal advice. If you require legal advice, you should consult with an attorney. Unless otherwise noted, HIPAA COW has not addressed all state pre-emption issues related to this Document. Therefore, this Document may need to be modified in order to comply with Wisconsin/State law.

LEGAL NOTICE: HIPAA Collaborative of Wisconsin Content and Liability Disclaimer

The HIPAA Collaborative of Wisconsin (HIPAA COW) shall not be responsible for any errors or omissions contained in materials provided by HIPAA COW. All information is provided on an "AS IS" basis.

HIPAA COW MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED (INCLUDING ANY WARRANTIES OF TITLE, NON-INFRINGEMENT AND IMPLIED WARRANTIES OF MERCHANT-ABILITY OR FITNESS FOR A PARTICULAR PURPOSE) REGARDING ANY INFORMATION CONTAINED IN ITS MATERIALS. THE USER OF THE MATERIALS SHALL ASSUME TOTAL RESPONSIBILITY AND RISK FOR THE USE OF THE MATERIALS.   IN NO EVENT SHALL HIPAA COW BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO ANY INFORMATION CONTAINED IN THE MATERIALS PROVIDED BY HIPAA COW, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW OR OTHERWISE.

The content of the materials provided by HIPAA COW is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that HIPAA COW is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Today's Host

Catherine M. Boerner, JD, CHC

President

Boerner Consulting, LLC

Boerner Consulting LLC

Objectives

- Provide a high-level overview of HIPAA
- Identify HIPAA Security Rule Requirements
- Identify Resources

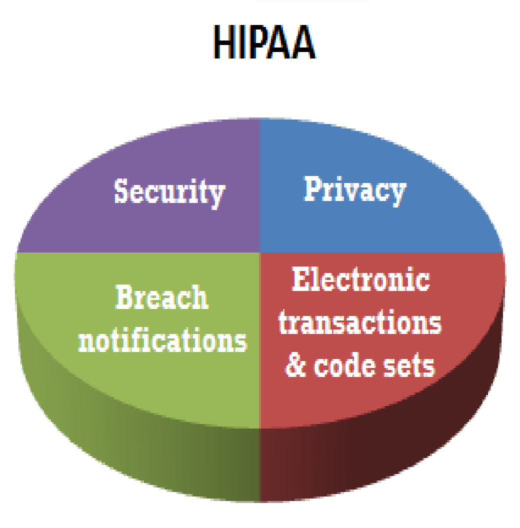
What is HIPAA?

HIPAA is an acronym for the Health Insurance Portability & Accountability Act of 1996 designed to create national standards to:

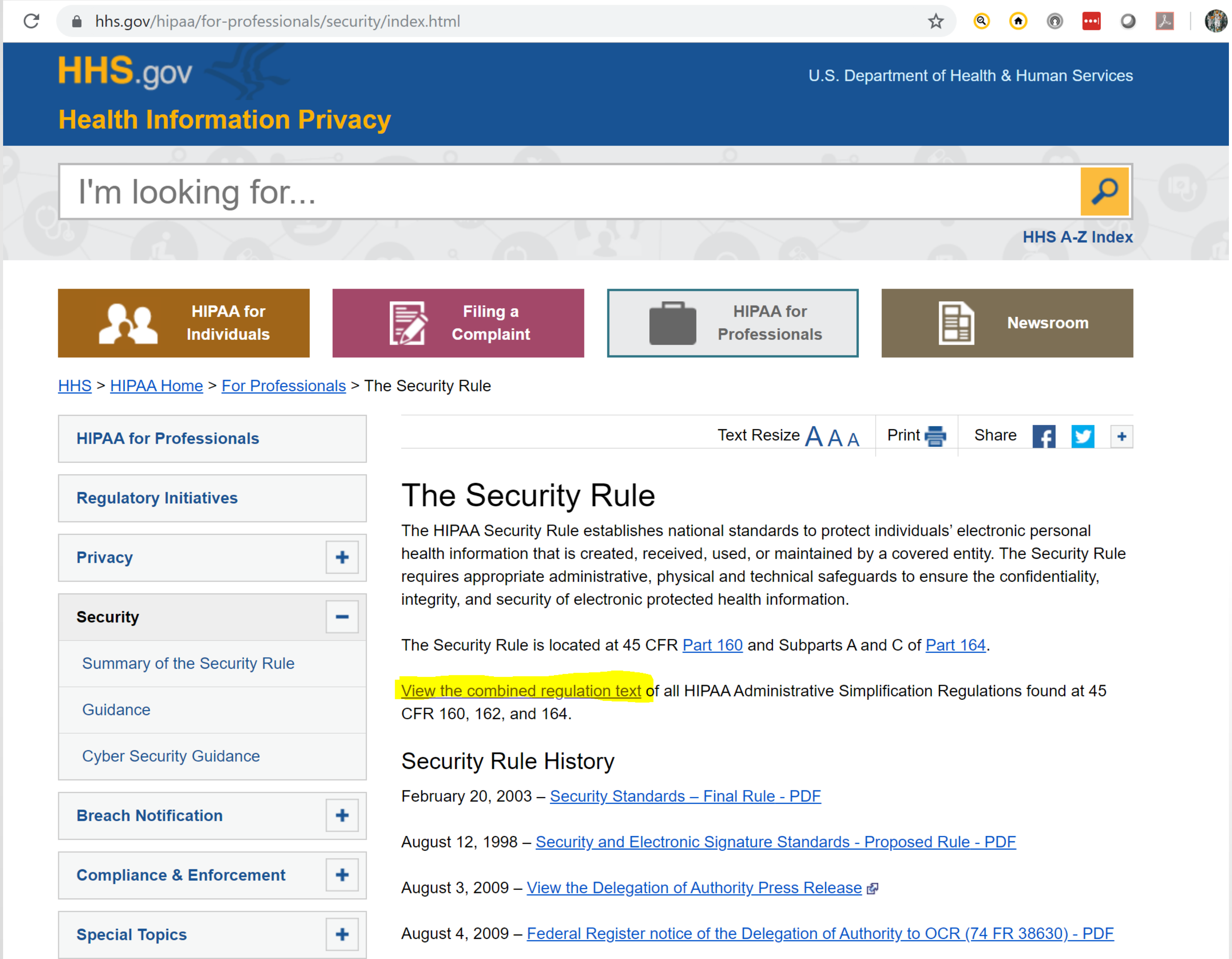
- Protect and enhance patient rights by better controlling and providing access to their health information;
- Establish nationwide protection of patient confidentiality, security of electronic systems, and standards for electronic transmission of health information;
- Improve the quality of health care;
- Improve the efficiency and effectiveness of health care delivery by building national standards

What is HIPAA?

- HIPAA is an acronym for the **H**ealth **I**nsurance **P**ortability & **A**ccountability **A**ct of 1996
- HIPAA consists of four key sections



Each section has separate requirements organizations must follow



HHS > HIPAA Home > For Professionals > The Security Rule

The Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

View the combined regulation text of all HIPAA Administrative Simplification Regulations found at 45 CFR 160, 162, and 164.

Security Rule History

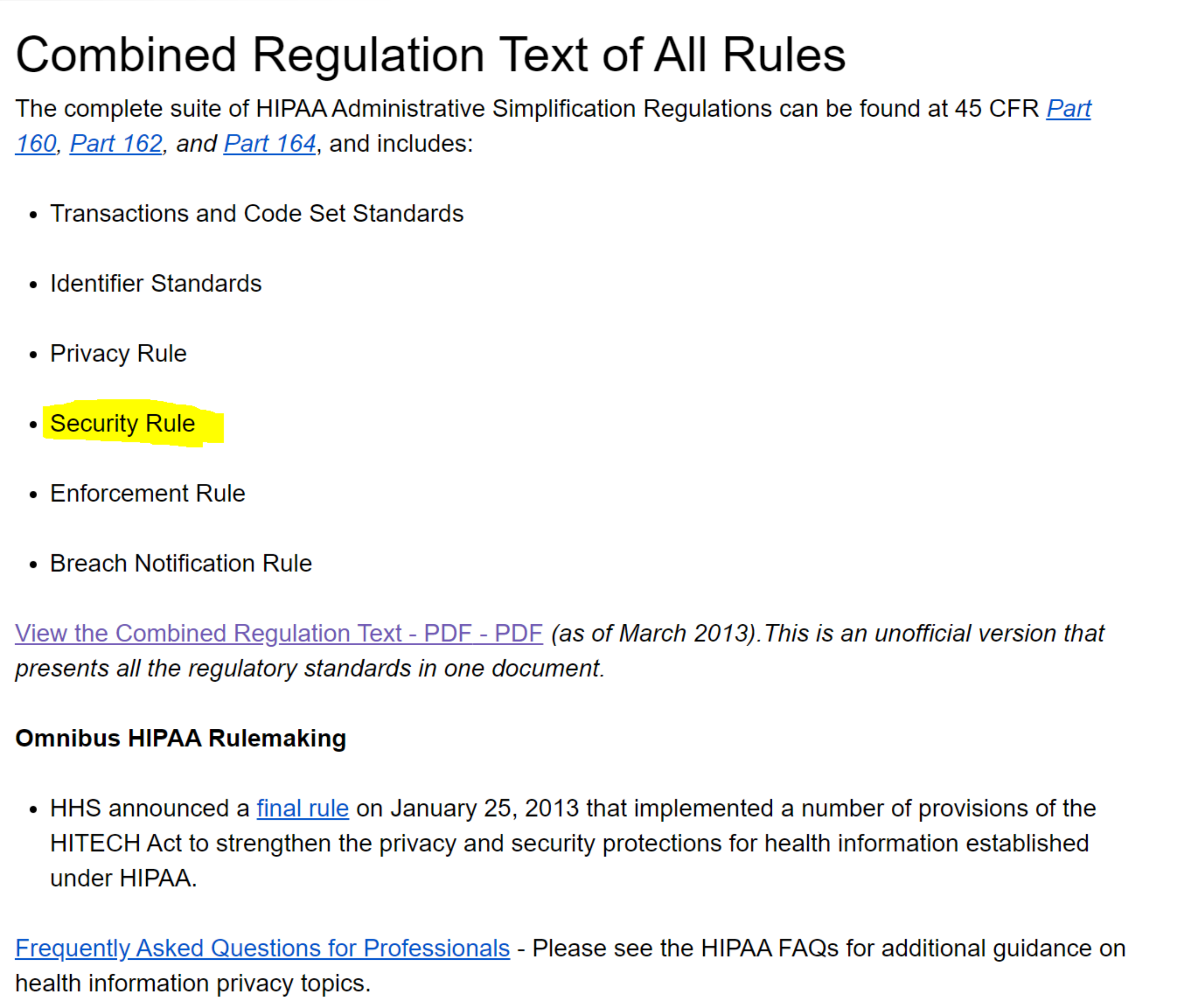
February 20, 2003 – Security Standards – Final Rule - PDF

August 12, 1998 – Security and Electronic Signature Standards - Proposed Rule - PDF

August 3, 2009 – View the Delegation of Authority Press Release

August 4, 2009 – Federal Register notice of the Delegation of Authority to OCR (74 FR 38630) - PDF

hipaacow.org®



Combined Regulation Text of All Rules

The complete suite of HIPAA Administrative Simplification Regulations can be found at 45 CFR *Part 160, Part 162, and Part 164*, and includes:

- Transactions and Code Set Standards
- Identifier Standards
- Privacy Rule
- Security Rule
- Enforcement Rule
- Breach Notification Rule

View the Combined Regulation Text - PDF - PDF *(as of March 2013).This is an unofficial version that presents all the regulatory standards in one document.*

Omnibus HIPAA Rulemaking

- HHS announced a final rule on January 25, 2013 that implemented a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA.

Frequently Asked Questions for Professionals - Please see the HIPAA FAQs for additional guidance on health information privacy topics.

hipaacow.org®

Who is covered by the Security Rule?

The Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits any health information in electronic form in connection with a transaction for which the Secretary of DHHS has adopted standards under HIPAA (the "**covered entities**") and to their **business associates**.

HIPAA Security Rule Seven Sections

I. General Rules (164.306)

II. Administrative Safeguards (164.308)

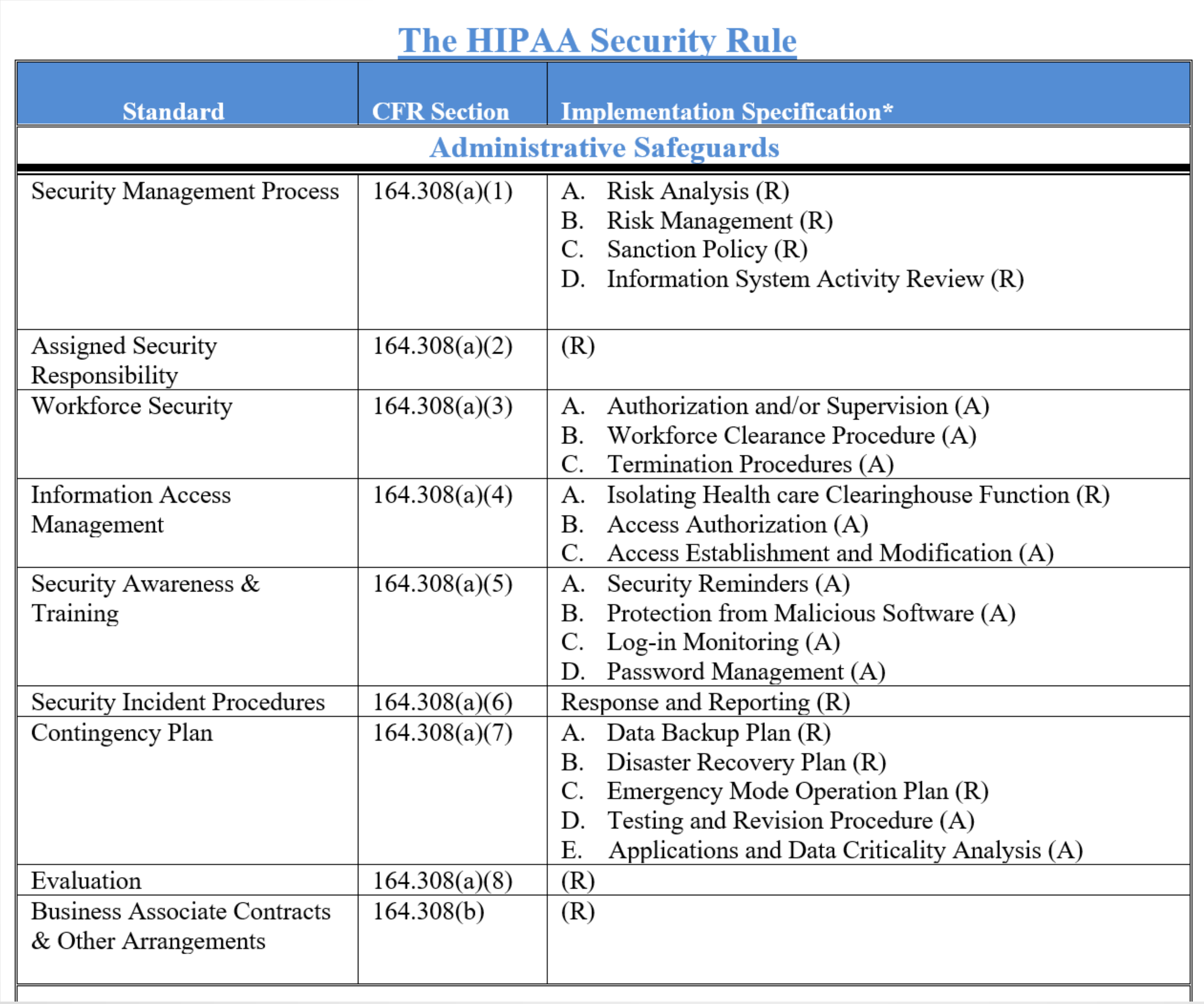
III. Technical Safeguards (164.310)

IV. Physical Safeguards (164.312)

V. Organizational Requirements (164.314)

VI. Policies and Procedures and Documentation Requirements (164.316)

VII. Compliance Dates for the initial implementation of the security standards (164.318) = **April 20, 2005**

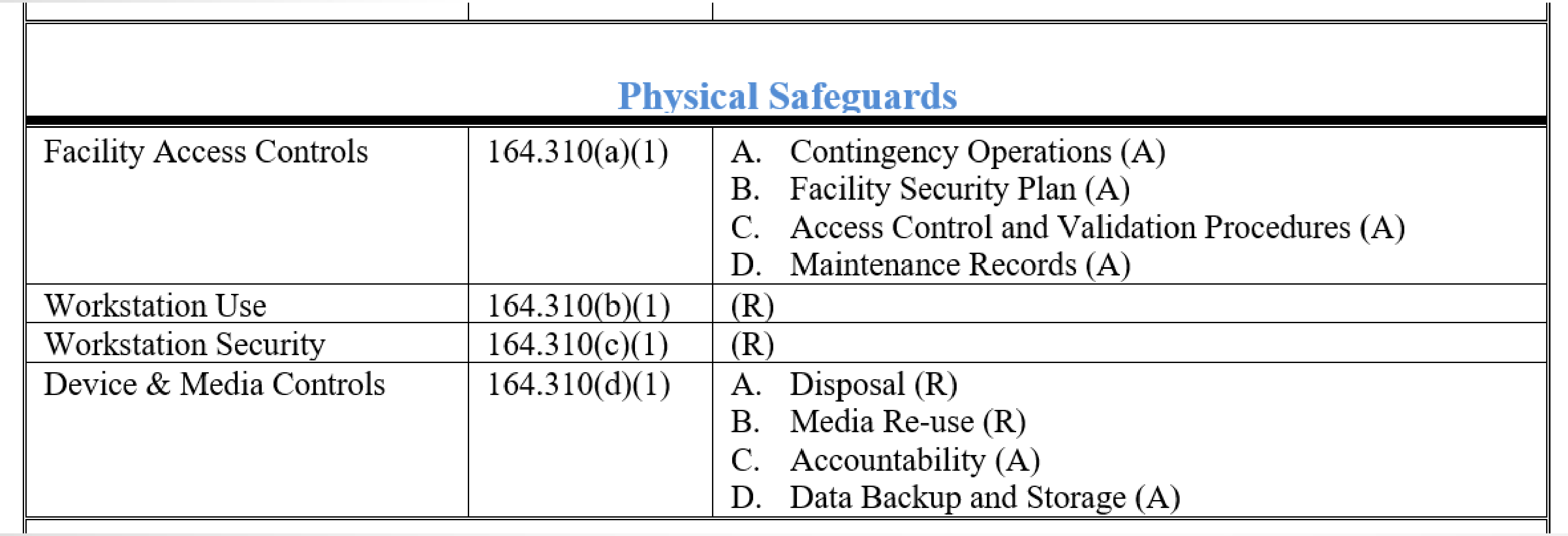


The HIPAA Security Rule

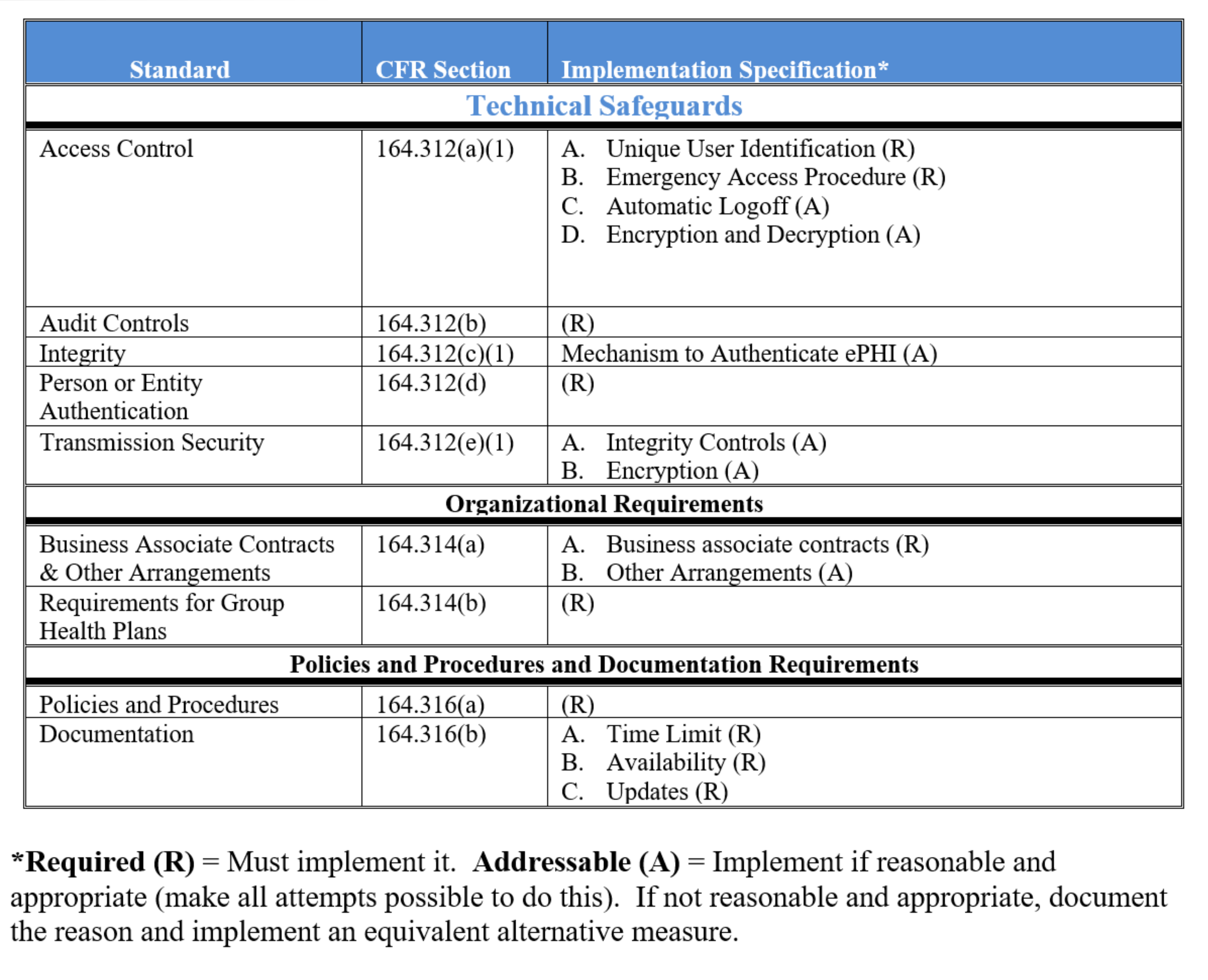
Standard	CFR Section	Implementation Specification*
Administrative Safeguards		
Security Management Process	164.308(a)(1)	A. Risk Analysis (R) B. Risk Management (R) C. Sanction Policy (R) D. Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	A. Authorization and/or Supervision (A) B. Workforce Clearance Procedure (A) C. Termination Procedures (A)
Information Access Management	164.308(a)(4)	A. Isolating Health care Clearinghouse Function (R) B. Access Authorization (A) C. Access Establishment and Modification (A)
Security Awareness & Training	164.308(a)(5)	A. Security Reminders (A) B. Protection from Malicious Software (A) C. Log-in Monitoring (A) D. Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	A. Data Backup Plan (R) B. Disaster Recovery Plan (R) C. Emergency Mode Operation Plan (R) D. Testing and Revision Procedure (A) E. Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts & Other Arrangements	164.308(b)	(R)

hipaacow.org®

HIPAA Security Rule



Physical Safeguards		
Facility Access Controls	164.310(a)(1)	A. Contingency Operations (A) B. Facility Security Plan (A) C. Access Control and Validation Procedures (A) D. Maintenance Records (A)
Workstation Use	164.310(b)(1)	(R)
Workstation Security	164.310(c)(1)	(R)
Device & Media Controls	164.310(d)(1)	A. Disposal (R) B. Media Re-use (R) C. Accountability (A) D. Data Backup and Storage (A)



Standard	CFR Section	Implementation Specification*
Technical Safeguards		
Access Control	164.312(a)(1)	A. Unique User Identification (R) B. Emergency Access Procedure (R) C. Automatic Logoff (A) D. Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate ePHI (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	A. Integrity Controls (A) B. Encryption (A)
Organizational Requirements		
Business Associate Contracts & Other Arrangements	164.314(a)	A. Business associate contracts (R) B. Other Arrangements (A)
Requirements for Group Health Plans	164.314(b)	(R)
Policies and Procedures and Documentation Requirements		
Policies and Procedures	164.316(a)	(R)
Documentation	164.316(b)	A. Time Limit (R) B. Availability (R) C. Updates (R)

***Required (R)** = Must implement it. **Addressable (A)** = Implement if reasonable and appropriate (make all attempts possible to do this). If not reasonable and appropriate, document the reason and implement an equivalent alternative measure.

HIPAA Security Rule Implementation

The requirements in each of these sections often overlap. The HIPAA COW Security Risk Toolkit attempts to logically sort the requirements so that organizations can focus on one category/or type of requirement at a time. I will follow this approach to discuss administrative, physical and technical safeguards that may be best addressed and implemented together to prevent revisiting an area.

Example:
System Access Policy and Procedure

45 CFR §164.308(a)(3)(i)	Workforce Security	Administrative
45 CFR §164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Administrative
45 CFR §164.308(a)(3)(ii)(B)	Workforce Clearance Procedures	Administrative
45 CFR §164.308(a)(3)(ii)(C)	Termination Procedures	Administrative
45 CFR §164.308(a)(4)(i)	Information Access Management	Administrative
45 CFR §164.308(a)(4)(ii)(B)	Access Authorization	Administrative
45 CFR §164.308(a)(4)(ii)(C)	Access Establishment and Modification	Administrative
45 CFR §164.308(a)(5)(ii)(D)	Password Management	Administrative
45 CFR §164.310(b)	Workstation Use	Physical
45 CFR §164.310(c)	Workstation Security	Physical
45 CFR §164.312(a)(1)	Access Control	Technical
45 CFR §164.312(a)(2)(i)	Unique User Identification	Technical
45 CFR §164.312(a)(2)(iii)	Automatic Logoff	Technical
45 CFR §164.312(d)	Person or Entity Authentication	Technical

hipaacow.org®

HIPAA Security Rule Safeguards

A. Risk Management & Risk Analysis
B. Contingency Plan
C. Data Management
D. Auditing
   i. User Audits
   ii. Log-in Monitoring
   iii. Malicious Software

HIPAA Security Rule Safeguards

E. HIPAA Oversight

- i. Assigned Security Responsibility
- ii. General Oversight
- iii. Training

F. Incidents

- i. Security Incident Response
- ii. Sanctions
- iii. Breach Notification

HIPAA Security Rule Safeguards

G. System Access

i. Roles

ii. Authorize

iii. Modify

iv. Terminate

v. Health Care Clearinghouse

vi. Passwords

vii. Workstation

viii. Auto Log-off

HIPAA Security Rule Safeguards

H. Business Associate (BA) / Subcontractors
I. Facility Access
J. Facility Maintenance
K. Disposal of Confidential Information
L. Technical Access Control
    i. Transmission Security
    ii. Encryption
    iii. Integrity
M. Group Health Plan

164.308(a)(1)(ii)(A-B);
164.308(a)(8)

1. Risk Management

- Risk Analysis
- Rank the threats & vulnerabilities
- Probability of Occurrence
- Potential Impact
- Write Risk Management procedures
- Periodically review

hipaacow.org®

164.308(a)(1)(ii)(A-B);
164.308(a)(8)

1. Risk Management

Q: What is the difference between Risk Analysis and Risk Management in the Security Rule?

A: **Risk analysis** is the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic protected health information (e-PHI) held by a covered entity, and the likelihood of occurrence. The risk analysis may include **taking inventory of all systems and applications that are used to access and house data, and classifying them by level of risk**.

hipaacow.org®

164.308(a)(1)(ii)(A-B);
164.308(a)(8)

1. Risk Management

(continue)

A thorough and accurate risk analysis would consider all relevant losses that would be expected if the **security measures** were not in place, including loss or damage of data, corrupted data systems, and anticipated ramifications of such losses or damage. **Risk management** is the actual implementation of security measures to sufficiently reduce an organization's risk of losing or compromising its e-PHI and to meet the general security standards.

Content created by Office for Civil Rights (OCR)

Content last reviewed on July 26, 2013

1. 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 or business associate.”

164.308a1iiA

164.308(a)(1)(ii)(A-B);
164.308(a)(8)

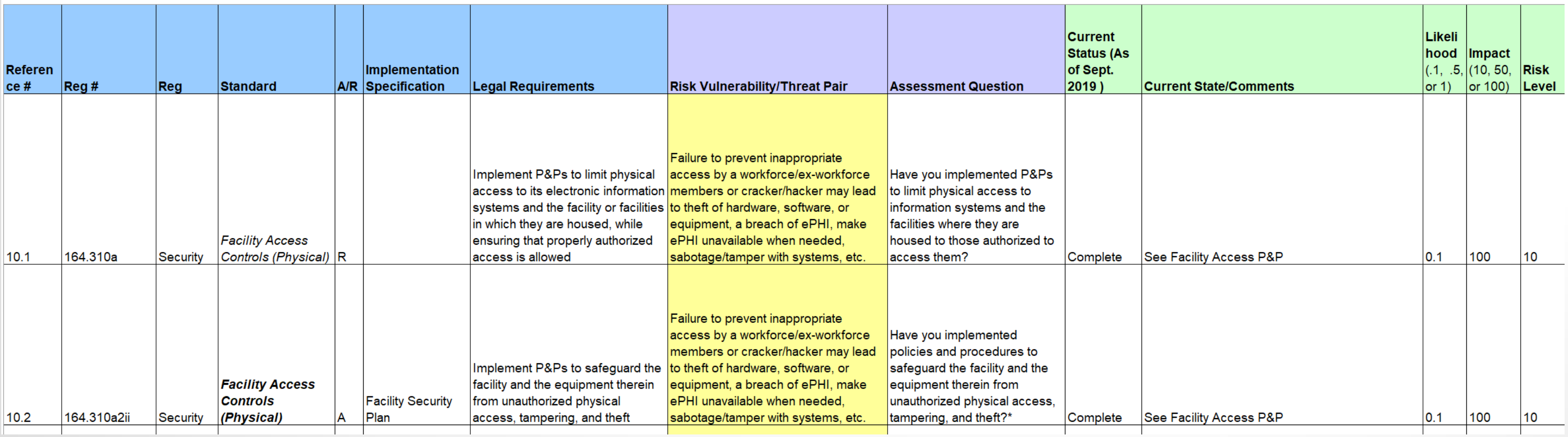
1. Risk Analysis

Where is the ePHI?

Taking inventory of all systems and applications that are used to access and house data, and classifying them by level of risk.

164.308(a)(1)(ii)(A-B);
164.308(a)(8)

1. Risk Analysis



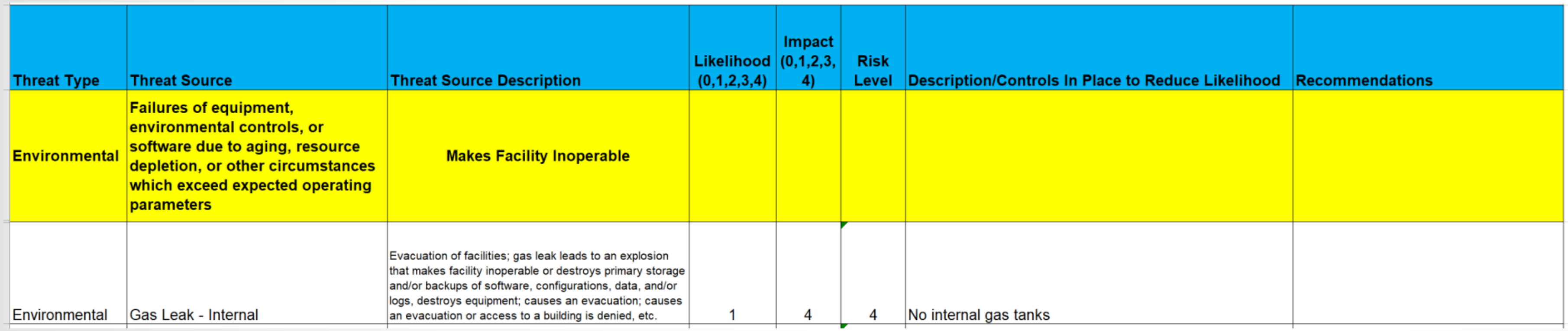
Reference #	Reg #	Reg	Standard	A/R	Implementation Specification	Legal Requirements	Risk Vulnerability/Threat Pair	Assessment Question	Current Status (As of Sept. 2019)	Current State/Comments	Likelihood (.1, .5, or 1)	Impact (10, 50, or 100)	Risk Level
10.1	164.310a	Security	*Facility Access Controls (Physical)*	R		Implement P&Ps to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed	Failure to prevent inappropriate access by a workforce/ex-workforce members or cracker/hacker may lead to theft of hardware, software, or equipment, a breach of ePHI, make ePHI unavailable when needed, sabotage/tamper with systems, etc.	Have you implemented P&Ps to limit physical access to information systems and the facilities where they are housed to those authorized to access them?	Complete	See Facility Access P&P	0.1	100	10
10.2	164.310a2ii	Security	***Facility Access Controls (Physical)***	A	Facility Security Plan	Implement P&Ps to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft	Failure to prevent inappropriate access by a workforce/ex-workforce members or cracker/hacker may lead to theft of hardware, software, or equipment, a breach of ePHI, make ePHI unavailable when needed, sabotage/tamper with systems, etc.	Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft?*	Complete	See Facility Access P&P	0.1	100	10

hipaacow.org®

164.308(a)(1)(ii)(A-B);
164.308(a)(8)

1. Risk Analysis

Threat Source List (Example)



Threat Type	Threat Source	Threat Source Description	Likelihood (0,1,2,3,4)	Impact (0,1,2,3, 4)	Risk Level	Description/Controls In Place to Reduce Likelihood	Recommendations
Environmental	**Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters**	**Makes Facility Inoperable**					
Environmental	Gas Leak - Internal	Evacuation of facilities; gas leak leads to an explosion that makes facility inoperable or destroys primary storage and/or backups of software, configurations, data, and/or logs, destroys equipment; causes an evacuation; causes an evacuation or access to a building is denied, etc.	1	4	4	No internal gas tanks	

Think through the type of threats:

- Environmental,
- Human,
- Natural Disaster
- Technology
- Other

1. 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 or business associate 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.”

164.308a1iiB

164.308(a)(7)(i);
164.308(a)(7)(ii)(B-E);
164.310(a)(2)(i-ii)

2. Contingency Plan

Goal: Restore access to ePHI ASAP

- Write and implement P&Ps to:
  - Respond to emergencies
    - Access to e-phi
    - Access to facilities
  - Restore lost ePHI
  - Periodically test & revise your Contingency Plans
  - Assess the relative criticality of applications & data

164.308(a)(7)(i);
164.308(a)(7)(ii)(B-E);
164.310(a)(2)(i-ii)

2. Contingency Plan

Goal: Restore access to ePHI ASAP

- Disaster Recovery Plan
- Emergency Mode Operations Plan
- Testing and Revision Procedures
- Applications and Data Criticality Analysis

hipaacow.org®

164.308(a)(7)(ii)(A);
164.310(d)(1);
164.310(d)(2)(iii-iv)

3. Data Management

Goal: no loss of ePHI

- Write & implement procedures to:
  - Backup ePHI
  - Secure equipment transportation
  - Hardware movement records

164.308(a)(1)(ii)(D);
164.308(a)(5)(ii)(B-C);
164.312(b)

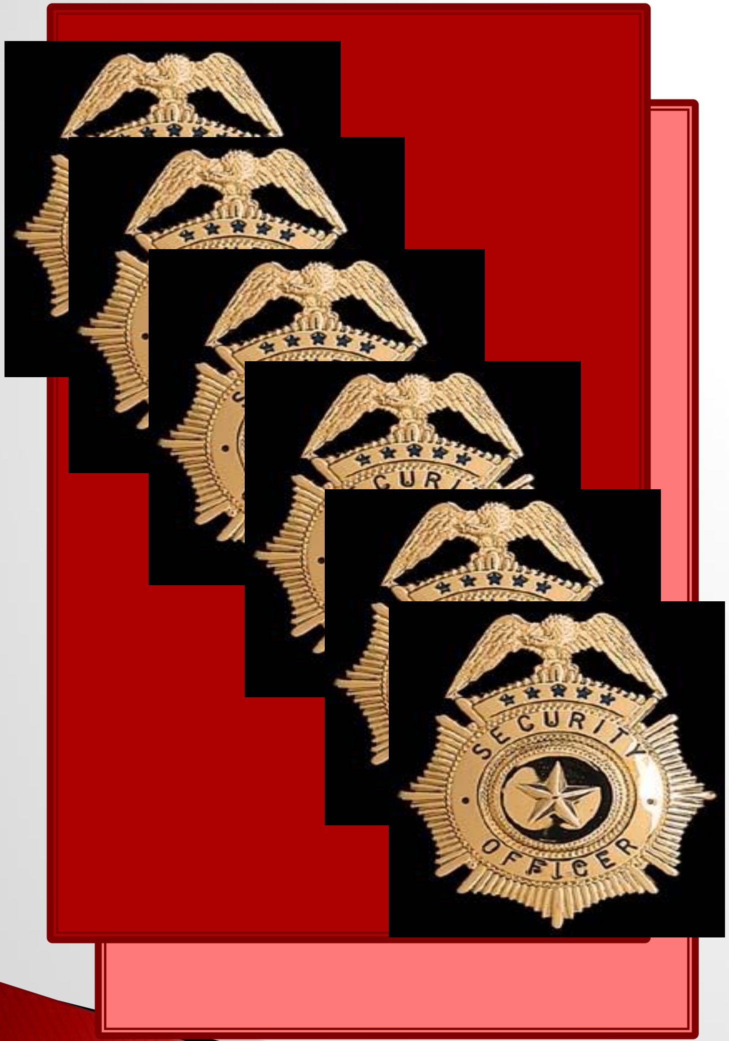
4. Auditing

- Have mechanisms to record and examine activity in information systems that contain or use ePHI
- Write & implement procedures to:
  - Regularly audit users’ access to ePHI
  - Monitor log-in attempts and report potential issues
  - Guard against, detect, and report viruses, Trojan horses, and worms

hipaacow.org®

5. HIPAA Oversight:

164.306(a-e)
164.308(a)(2);
164.316(a-b)



- Write & implement procedures to:
  - Monitor security measures
  - Save/store all documentation for at least 6 years
  - Make available to users
  - Periodically update/review
- Identify a Security Official (e.g. Security Officer)

164.308(a)(5)(i);
164.308(a)(5)(ii)(A)

6. Training

- Security awareness training program required for all workforce, and to document it
- Provide periodic security reminders and updates
- Targeted Training

Make security a part of their daily activities

7. Incidents

164.308(a)(1)(i);
164.308(a)(6)(i-ii);
164.308(a)(1)(ii)(C);
13402(a,b,e); 13406

- Document a Security Incident Response plan
  - Prevent
  - Identify & respond
  - Contain
  - Mitigate
  - Document incidents & outcomes
- Require reporting of breaches of "unsecured ePHI"
  - If you are a BA, report breaches of "unsecured ePHI" to the Covered Entity
  - Notify the individual, Secretary, and media, as required
- Apply consistent sanctions

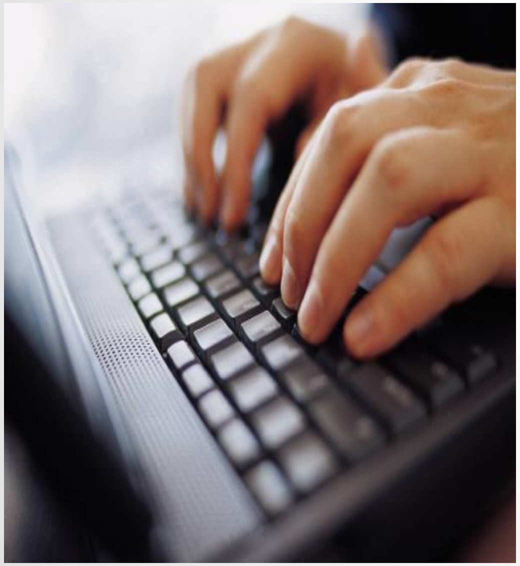
8. System Access

164.308(a)(3)(i); 164.308(a)(3)(ii)(A-C);
164.308(a)(4)(i); 164.308(a)(4)(ii)(A-C);
164.312(a)(2)(iii); 164.308(a)(5)(ii)(D);
164.312(a)(2)(i); 164.312(d); 164.310(b-c)

Write & implement procedures:

A. **Authorization**:
   - Appropriate minimum necessary access by level
   - Method to authorize access
   - Only those who need access
   - *Modify* when role changes
   - *Terminate* when leaving or not longer required
   - Supervise workforce

8. System Access, continued



B. **Auto Log-off**

- Automatically terminate access to ePHI systems after a predetermined time of inactivity.

C. **Health Care Clearinghouse**

- Prevent access to ePHI by the larger organization (Covered Entity)

8. System Access, continued

D. **Passwords**

- Password standards
  - Creation
  - Change Frequency (30,60,90 days)
  - Structure (Length, special characters, numbers)
- Unique User IDs (no sharing)
- Person or Entity Authentication

8. System Access, continued

E. **Workstation**

- Explain how, when, and where workstations, portable devices, etc. may be used and who may use them
- Describe where workstations, portable devices, etc. may be located & how to protect them from unauthorized users

13404; 13408; 13401(a); 164.308(b)(1-4); 164.314(a)(1); 164.314(a)(2)(i-ii)

9. Business Associate Agreements (BAAs)

- Write and implement a P&P to obtain HIPAA Privacy, Security, & HITECH compliant BAAs
  - Have BAAs in place with vendors that provide data transmission of PHI to your organization (HIEO, RHIO, E-prescribing gateway)
- Maintain copies of BAAs
- BAA Incident Reporting Process
- If your organization is a:
  - *Governmental entity* and have BAAs with other governmental entities, require they sign a memorandum of understanding
  - *BA*, write & implement a P&P to follow BAA requirements

164.310(a);
164.310(a)(2)(ii-iii)

10. Facility Access

- Write & implement P&Ps to:
  - Limit physical access to ePHI systems and storage areas/facilities to only those that need access
  - Safeguard the facility and the equipment from unauthorized physical access, tampering & theft
  - Control & validate access to facilities based on role, including visitors.

164.310(a)(2)(iv)

11. Facility Maintenance

- Write & implement P&Ps to:
  - Document repairs & changes made to buildings (related to security)

164.310(d)(2)(i-ii)

12. ePHI Disposal

- Write & implement P&Ps to:
  - Destroy ePHI on hardware or other electronic media no longer being used
  - Remove ePHI from electronic media before being used by anyone else (internally or externally)

hipaacow.org®

13. Technical Access Control: Encryption & Integrity

164.312(e)(1);
164.312(a)(2)(iv);
164.312(e)(2)(i-ii);
164.312c(1-2)

- Write & implement P&Ps to:
  - Prevent unauthorized access to ePHI during transmission over electronic communication networks
  - Prevent ePHI from being improperly changed or destroyed
- Implement a way(s) to:
  - Encrypt & decrypt ePHI at rest & in transit
  - Confirm that ePHI has not been altered or destroyed in an unauthorized manner
  - Ensure that electronically transmitted ePHI is not improperly modified without detection until disposed

14. Group Health Plans

- If you sponsor a self-insured health plan, include in your plan documents that you reasonably & appropriately safeguard ePHI that you create, receive, maintain, or transmit on behalf of the group health plan.
  - Include that you report security incidents to the group health plan

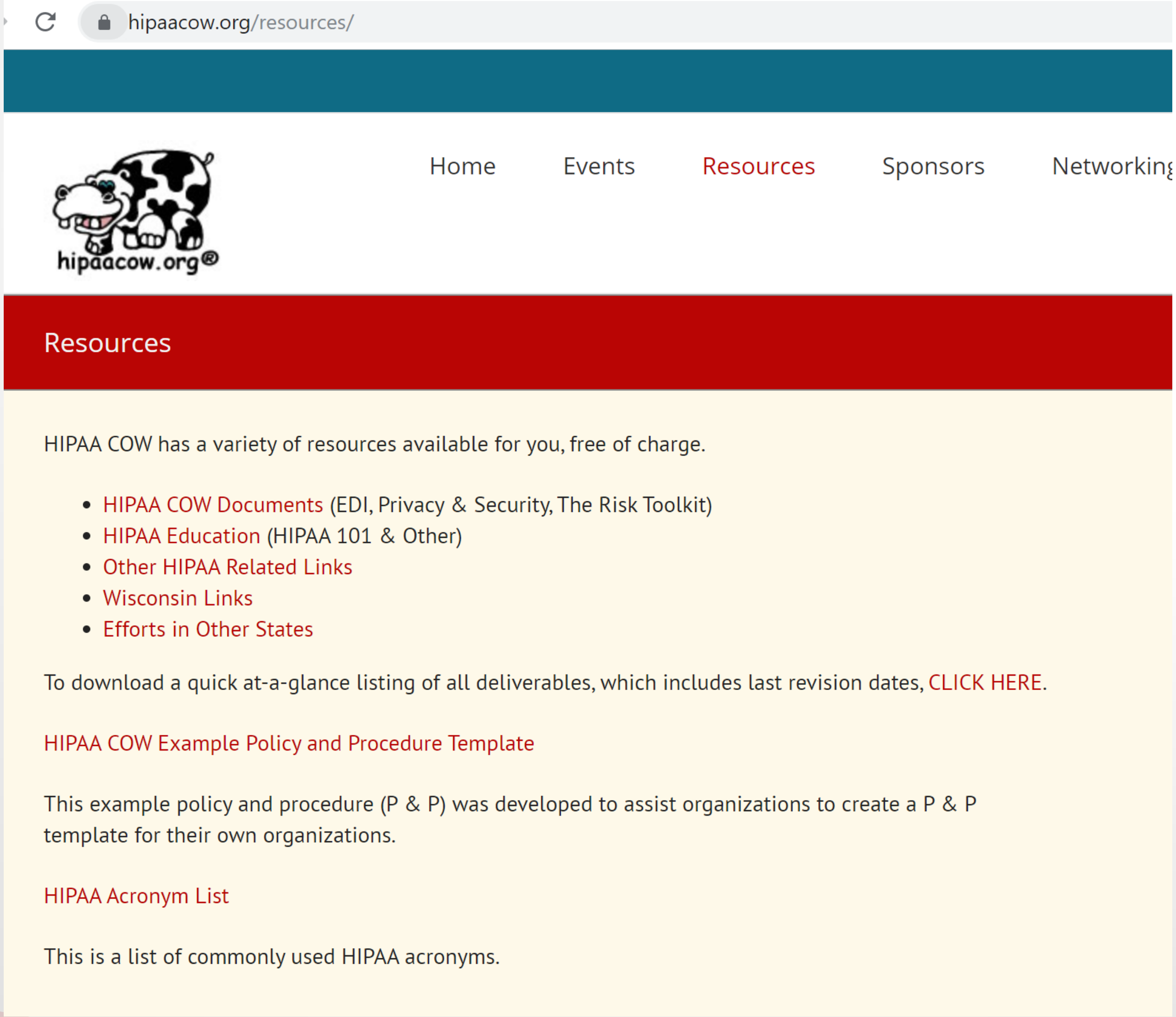
HIPAA ENFORCEMENT PENALTIES

- May be imposed to the Organization and an Individual. Four Tiers:
  - Unknown and even with due diligence could not have been known $100-$50,000
  - Due to general failure to comply but not intentional failure $1,000-$50,000
  - Due to intentional failure to comply and was corrected $10,000-$50,000
  - Due to intentional failure to comply and was NOT corrected $50,000

Initial Security Compliance Checklist

- Appoint a Security Officer
- Establish and maintain Security Policies & Procedures
- Auditing
- Develop and Maintain Workforce Security Training, Education, and Awareness Program
- Develop Process for Responding to Security incidents
- Develop Workforce Sanctions Process or Coordinate with Human Resources Corrective Action Process

Resources



hipaacow.org/resources/

Home Events Resources Sponsors Networking

Resources

HIPAA COW has a variety of resources available for you, free of charge.

- HIPAA COW Documents (EDI, Privacy & Security, The Risk Toolkit)
- HIPAA Education (HIPAA 101 & Other)
- Other HIPAA Related Links
- Wisconsin Links
- Efforts in Other States

To download a quick at-a-glance listing of all deliverables, which includes last revision dates, CLICK HERE.

HIPAA COW Example Policy and Procedure Template

This example policy and procedure (P & P) was developed to assist organizations to create a P & P template for their own organizations.

HIPAA Acronym List

This is a list of commonly used HIPAA acronyms.

Resources – *CONTINUED*

- HHS Summary of the Security Rule

  https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

- Security Rule Guidance Material

  https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

- HHS Frequently Asked Questions

  https://www.hhs.gov/hipaa/for-professionals/faq/index.html

Resources – *CONTINUED*

- HHS Office for Civil Rights

  http://www.hhs.gov/ocr/office/index.html

- HHS OCR Audit Program

  https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

- OCR Enforcement Highlights

  https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

hipaacow.org®

Thank You!

Thank you for viewing this webinar. If you have any comments or feedback, please feel free to email us at admin2@hipaacow.org.

Visit our website at hipaacow.org!!

hipaacow.org®

“Like Us” on facebook

“Follow Us” on LinkedIn