Disclaimer

The topics taught here are for the sole purpose of providing clinical business-related compliance to healthcare providers. Any transference of this information to other purposes are at the risk of the individual's discretion. The presenter is an investor in the Best Practices Academy and ChiroArmor/ClinicArmor. The Best Practices Academy and ChiroArmor/ClinicArmor denies responsibility or liability for any erroneous opinions, analysis, and coding misunderstandings on behalf of individuals undergoing this course.

This presentation was current at the time it was published or uploaded as a course. Medicare policy changes frequently so links to the source documents have been provided within the document for your reference. We have based the majority of this program on the guidelines set forth by the OSHA, OCR, HHS, CMS, NCQA, URAC, AAAHC, AHRQ, DOJ, and other agencies involved in health care standards and research dissemination, as it relates to the healthcare. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

No legal advice is given in this program, and we encourage you to refer any such questions to your healthcare attorney.

HIPAA HISTORY

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Uniform standards and requirements for the electronic transmission of certain health information
- Required an approach that would not compromise privacy as health information became more accessible
- Health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with a transaction for which HHS has adopted a standard to maintain reasonable and appropriate administrative, physical, and technical safeguards

Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), part of the American Recovery and Reinvestment Act of 2009 (ARRA)

- Nationwide adoption and standardization of health information technology (health IT) to support the electronic sharing of clinical data
- Created financial incentives for health IT use among health care practitioners by providing funding for investing in health IT infrastructure, purchasing certified electronic health records (EHRs)
- HITECH Act also introduced substantial changes to the HIPAA regulations by mandating stronger safeguards for the privacy and security of ePHI

In 2013, the Department issued the final rule "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules HITECH Act

Extended the application of the Security Rule's administrative, physical, and technical safeguards requirements, as well as the rule's policies and procedures and documentation requirements, to **business associates in the same manner as the requirements apply to covered entities**, making those business associates civilly and criminally liable for violations of the Security Rule.

2013 Omnibus Rule modified the Security Rule to clarify that a covered entity is not required to obtain satisfactory assurance from a business associate that is a subcontractor

Rather, the business associate of the covered entity must obtain the required satisfactory assurances from the subcontractor to protect the security of ePHI.

OCR Cybersecurity Experience the past 10 years has led to an enhancement to the HIPAA Security Rule

What is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

https://www.cisa.gov/news-events/news/what-cybersecurity

Healthcare sector is particularly vulnerable to cybersecurity risks

HHS tracks large data breaches through its Office for Civil Rights (OCR), whose data shows a 93% increase in large breaches reported from 2018 to 2022 (369 to 712), with a 278% increase in large breaches reported to OCR involving ransomware from 2018 to 2022.

DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office of the Secretary
45 CFR Parts 160 and 164
RIN 0945–AA22

HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information

898 Federal Register / Vol. 90, No. 3 / Monday, January 6, 2025 / Proposed Rules

https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html

Purpose:

To modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule to strengthen cybersecurity protections for electronic protected health information (ePHI)

What does this Proposed Rule entail?

Responsibility on Providers has Increased…

- Security management
- Regular monitoring and review of information system activity
- Information access management
- Security awareness and training
- Contingency planning
- Encryption
- Authentication

OCR's Experience: Regulated entities are not consistently complying with the Security Rule's requirements

What is at stake?

A failure to implement adequate security measures may lead to: financial loss; reputational harm for affected individuals and affected regulated entities; privacy loss; and safety concerns.

Cyber incidents have led to extended care disruptions

Results in:

- multi-week outages
- patient diversion to other facilities
- strain on acute care provisioning and capacity
- cancelled medical appointments
- non-rendered services
- delayed medical procedures
- put patients' safety at risk
- impact local and surrounding communities availability of the local emergency department, etc. for life-saving care.

PHI is immutable… individual's date and location of birth and their health history will not change

PHI can continue to be exploited throughout an individual's lifetime, making PHI likely to be far more valuable than an individual's credit card information

Implications of such harms are far greater in the health care sector because of their potential to adversely affect an individual's health or quality of life, or even to cost an individual their life.

OCR Experience…

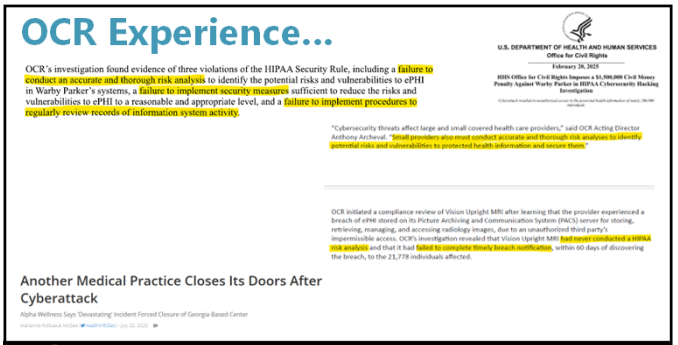
A 2020 cyberattack on a large integrated academic health system, attributed to **malicious software embedded in an email attachment** opened by an employee on their laptop, affected more than 5,000 end-user devices across 1,300 servers and led to revenue losses of more than $63 million.

Though the health care provider's EHR was not infected, it elected to shut the EHR down proactively. Ultimately, the covered entity "experienced **39 days of downtime** in outpatient imaging.

OCR Experience…

Ransomware attack on an academic level 1 trauma center caused it to go **without access to its EHR for 25 days**, and the attack affected 5,000 computers and destroyed the trauma center's electronic information systems that contained ePHI. The hospital **lost access to its EHR, internet, and intranet**, which also "**removed functionality** of hospital phones, [EHR] integrated office and surgical scheduling, access to digitized radiology studies, and network account access through local and remote computers.

OCR Experience…



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

February 20, 2025

HHS Office for Civil Rights Imposes a $1,500,000 Civil Money Penalty Against Warby Parker in HIPAA Cybersecurity Hacking Investigation

OCR's investigation found evidence of three violations of the HIPAA Security Rule, including a failure to conduct an accurate and thorough risk analysis to identify the potential risks and vulnerabilities to ePHI in Warby Parker's systems, a failure to implement security measures sufficient to reduce the risks and vulnerabilities to ePHI to a reasonable and appropriate level, and a failure to implement procedures to regularly review records of information system activity.

"Cybersecurity threats affect large and small covered health care providers," said OCR Acting Director Anthony Archeval. "Small providers also must conduct accurate and thorough risk analyses to identify potential risks and vulnerabilities to protected health information and secure them."

OCR initiated a compliance review of Vision Upright MRI after learning that the provider experienced a breach of ePHI stored on its Picture Archiving and Communication System (PACS) server for storing, retrieving, managing, and accessing radiology images, due to an unauthorized third party's impermissible access. OCR's investigation revealed that Vision Upright MRI had never conducted a HIPAA risk analysis and that it had failed to complete timely breach notification, within 60 days of discovering the breach, to the 21,778 individuals affected.

Another Medical Practice Closes Its Doors After Cyberattack

Alpha Wellness Says 'Devastating' Incident Forced Closure of Georgia-Based Center

Justification for This Proposed Rulemaking

A. Strong Security Standards Are Essential to Protecting the Confidentiality, Integrity, and Availability of ePHI and Ensuring Quality and Efficiency in the Health Care System

B. The Health Care Environment Has Changed Since the Security Rule Was Last Revised and Will Continue To Evolve

C. Regulated Entities' Compliance With the Requirements of the Security Rule Is Inconsistent

D. It Is Reasonable and Appropriate To Strengthen the Security Rule To Address the Changes in the Health Care Environment and Clarify the Compliance Obligations of Regulated Entities

Security Rule: Applies only to electronic PHI (ePHI), which is transmitted by or maintained in electronic media

Initially published in 2003 and most recently revised in 2013.

Since its publication, there have been **significant changes to the environment** in which health care is provided and how the health care industry operates.

Almost every stage of modern health care relies on stable and secure computer and network technologies

Appointment scheduling, prescription orders, telehealth visits, medical devices, patient records, medical and pharmacy claims submissions and billing, insurance coverage verifications, payroll, facilities access and management, internal and external communications, and clinician resources.

Many regulated entities have been slow to strengthen their security measures to protect ePHI and their information systems…

For example, regulated entities continue to **rely on legacy systems and software that are unsupported by manufacturers**, which means that the manufacturers **no longer provide security** patches or other updates to address security threats and vulnerabilities.

Example: Have you upgraded to Windows 11?

Microsoft stops supporting Windows 10 on October 14, 2025, at which point technical assistance and security updates will no longer be provided for most editions. However, Microsoft is offering an Extended Security Updates (ESU) program for Windows 10 Home and Pro users, which will extend security updates until October 2026, for a fee.

Do you have a "Basic EHR" or is your EHR Certified?

Health IT Certification Program maintained by the Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology (ASTP/ONC) sets minimum requirements for certified health IT, including criteria that pertain to cybersecurity.

https://chpl.healthit.gov/#/search

Regulatory Compliance

Certified EHRs are required for participation in federal health programs like the Medicare Promoting Interoperability Program and the Merit-based Incentive Payment System (MIPS), ensuring compliance with federal laws such as HIPAA and the HITECH Act.

Basic EHRs may not meet these regulatory requirements.

OCR Statement: "Regulated entities also may want to consider adoption of certified health IT because it could contribute to compliance with the Security Rule."

https://chpl.healthit.gov/#/search

Adoption of Secure Patient Portals

86% Hospitals and Medical Clinics

What about AI?

New technologies come with increased risks and vulnerabilities to ePHI and the information systems that create, receive, maintain, or transmit it…

HHS AI Task Force has been assigned to develop a strategic plan that includes policies and frameworks on responsible deployment and use of AI and AI-enabled technologies.

Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 defined AI to include the following:

Artificial Intelligence (AI)

- Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
- An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
- An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
- A set of techniques, including machine learning, that is designed to approximate a cognitive task.
- An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

"technologies have the potential to drive innovation, increase market competition, and vastly improve care for patients and populations."

Experts anticipate that AI "will ultimately pioneer the malicious use of 'Offensive AI'—highly sophisticated and malicious attack code—[that] will be able to mutate itself as it learns about its environment, and to expertly compromise systems with minimal chance of detection."

Generative AI

A type of artificial intelligence that learns patterns from massive datasets to create entirely new content, such as text, images, audio, video, or code, in response to a user's prompt.

Publicly available generative AI tools, such as ChatGPT, are not secure and may share your information.

"uses of generative AI by regulated entities, including the training of AI models on patient data, could result in impermissible uses and disclosures, including exposure to bad actors that can exploit the information."

AI Software is defined as a part of the Technology Asset Inventory and should be included in your risk analysis.

Certified EHRs are under regulations which require such health IT developers to provide greater transparency about the design, development, training, evaluation, and use of such predictive decision support interventions DSIs.

I have a small practice, are there different rules for me?

Size does not matter…

"In fact, smaller regulated entities may also be the target of, or adversely affected by, cybercrime, partly because of the **interconnectedness of health care** and partly because they are **less likely to have invested in cybersecurity, making them easier targets**.

"Thus, small health care providers "are at the greatest risk of a breach."

"…we believe that small and rural health care providers have both the **need to comply** with the proposals in this NPRM and the **capability of doing so**."

Failure to invest adequate resources in cybersecurity infrastructure, complying with standards and implementation specifications of HIPAA.

"14 percent of covered entities and 17 percent of business associates were "substantially fulfilling their regulatory responsibilities to safeguard ePHI they [held] through risk analysis activities."

"there is no such thing as a totally secure system that carries no risks to security."

"However, we also made clear that a covered entity is **required to implement adequate security measures** and that cost was but one factor for a covered entity to consider when determining what constituted appropriate security measures."

Security Rule Update Addresses:

- Significant changes in technology.
- Changes in breach trends and cyberattacks.
- HHS' Office for Civil Rights' (OCR's) enforcement experience.
- Other guidelines, best practices, methodologies, procedures, and processes for protecting ePHI.
- Court decisions that affect enforcement of the Security Rule.

Security Rule's standards and implementation specifications with new proposals and clarifications, including:

- Remove the distinction between "required" and "addressable" implementation specifications and make all implementation specifications required with specific, limited exceptions.
- Require written documentation of all Security Rule policies, procedures, plans, and analyses.
- Update definitions and revise implementation specifications to reflect changes in technology and terminology.
- Add specific compliance time periods for many existing requirements.
- Require the development and revision of a technology asset inventory and a network map that illustrates the movement of ePHI throughout the regulated entity's electronic information system(s) on an ongoing basis, but at least once every 12 months and in response to a change in the regulated entity's environment or operations that may affect ePHI.

Security Rule's standards and implementation specifications with new proposals and clarifications, including:

- Require greater specificity for conducting a risk analysis. New express requirements would include a written assessment that contains, among other things:
  - A review of the technology asset inventory and network map.
  - Identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI.
  - Identification of potential vulnerabilities and predisposing conditions to the regulated entity's relevant electronic information systems
  - An assessment of the risk level for each identified threat and vulnerability, based on the likelihood that each identified threat will exploit the identified vulnerabilities.
- Require notification of certain regulated entities within 24 hours when a workforce member's access to ePHI or certain electronic information systems is changed or terminated.

Security Rule's standards and implementation specifications with new proposals and clarifications, including:

- Strengthen requirements for planning for contingencies and responding to security incidents. Specifically, regulated entities would be required to, for example:
  - Establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours.
  - Perform an analysis of the relative criticality of their relevant electronic information systems and technology assets to determine the priority for restoration.
  - Establish written security incident response plans and procedures documenting how workforce members are to report suspected or known security incidents and how the regulated entity will respond to suspected or known security incidents.
  - Implement written procedures for testing and revising written security incident response plans.
- Require regulated entities to conduct a compliance audit at least once every 12 months to ensure their compliance with the Security Rule requirements.

Security Rule's standards and implementation specifications with new proposals and clarifications, including:

- Require that business associates verify at least once every 12 months for covered entities (and that business associate contractors verify at least once every 12 months for business associates) that they have deployed technical safeguards required by the Security Rule to protect ePHI through a written analysis of the business associate's relevant electronic information systems by a subject matter expert and a written certification that the analysis has been performed and is accurate.
- Require encryption of ePHI at rest and in transit, with limited exceptions.
- Require regulated entities to establish and deploy technical controls for configuring relevant electronic information systems, including workstations, in a consistent manner. New express requirements would include:
  - Deploying anti-malware protection.
  - Removing extraneous software from relevant electronic information systems.
  - Disabling network ports in accordance with the regulated entity's risk analysis.

Security Rule's standards and implementation specifications with new proposals and clarifications, including:

- Require that business associates verify at least once every 12 months for covered entities (and that business associate contractors verify at least once every 12 months for business associates) that they have deployed technical safeguards required by the Security Rule to protect ePHI through a written analysis of the business associate's relevant electronic information systems by a subject matter expert and a written certification that the analysis has been performed and is accurate.
- Require encryption of ePHI at rest and in transit, with limited exceptions.
- Require regulated entities to establish and deploy technical controls for configuring relevant electronic information systems, including workstations, in a consistent manner. New express requirements would include:
  - Deploying anti-malware protection.
  - Removing extraneous software from relevant electronic information systems.
  - Disabling network ports in accordance with the regulated entity's risk analysis.

Security Rule's standards and implementation specifications with new proposals and clarifications, including:

- Require the use of multi-factor authentication, with limited exceptions.
- Require vulnerability scanning at least every six months and penetration testing at least once every 12 months.
- Require network segmentation.
- Require separate technical controls for backup and recovery of ePHI and relevant electronic information systems.
- Require regulated entities to review and test the effectiveness of certain security measures at least once every 12 months, in place of the current general requirement to maintain security measures.
- Require business associates to notify covered entities (and subcontractors to notify business associates) upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.
- Require group health plans to include in their plan documents requirements for their group health plan sponsors to: comply with the administrative, physical, and technical safeguards of the Security Rule…

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

Updates to Definitions

Definition of "Electronic Media"

Electronic storage material: Media which data can be recorded, maintained, or processed. This includes, but is not limited to, hard drives, removable media, magnetic tape, optical disk, and any other form of digital memory or storage.

Transmission media: used to exchange information already in electronic storage material. Transmission media includes, but is not limited to, the internet, extranet or intranet, leased lines, dial-up lines, private and public networks, and the physical movement of removable/transportable electronic storage material.

Data is either at rest, in transit, or in process.

Vulnerability resides in these three levels.

PART 164—SECURITY AND PRIVACY

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

Definition of "Access"

The Department proposes to **expand the list of activities** (i.e., activities are reading, writing, modifying, communicating data/information, or otherwise using any component of an information system) that should be considered under the term by adding the activities of "deleting" and "transmitting."

The Department also proposes to replace "system resource" with "component of an information system" to rely on an already defined term, "information system."

The proposed modification would clarify that the term includes any and all components of an information system and an information system as a whole.

Definition of "Administrative, Safeguards"

Administrative actions and related policies and procedures **to manage** the selection, development, implementation, and maintenance (including updating and modifying) of **security measures** to protect electronic protected health information, and **to manage the conduct** of the covered entity's or business associate's workforce in relation to the protection of that information.

Definition of "Authentication"

Corroboration that either a person or technology asset is the one they are claiming to be.

Definition of "Availability"

The property that data or information is accessible and usable upon demand by not only an authorized person or an authorized technology asset.

Definition of "Confidentiality"

The property that data or information is not made available or disclosed to unauthorized persons, **technology assets, or processes**.

Definition of "Deploy"

To configure technology for use and implement such technology.

Definition of "Electronic Information System"

Interconnected set of electronic information resources under the **same direct management control** that shares common functionality.

An electronic information system generally includes technology assets, such as hardware, software, electronic media, information, and data.

Applications are now regarded as software and not a technology asset – moving it to the regulatory requirements of an Information System.

EHR systems were previously regarded as "technology assets".

Encryption

The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Definition of "Facilities"

The physical premises and the interior and exterior of a building(s).

Definition of "Implement"

To put into effect and be in use, operational, and function as expected throughout the covered entity or business associate.

Definition of "Information System"

Interconnected set of information resources under the same direct management control that shares common functionality. An information system generally includes hardware, software, information, data, communications, **and people**.

Integrity

The property that data or information have not been altered or destroyed in an unauthorized manner.

Definition of "Malicious Software"

"Software or firmware intended to perform an **unauthorized action or activity** that will have adverse impact on an electronic information system and/or the confidentiality, integrity, or availability of electronic protected health information.

Examples include but are not limited to viruses, worms, Trojan horses, spyware, and some forms of adware.

Definition of "Multi-Factor Authentication" (MFA)

Authentication of the user's identity through verification of at least two of the following three categories:

1. Information known by the user, including but not limited to a password or personal identification number (PIN).
2. Item possessed by the user, including but not limited to a token or a smart identification card.
3. Personal characteristic of the user, including but not limited to fingerprint, facial recognition, gait, typing cadence, or other biometric or behavioral characteristics.

Definition of "Password"

Confidential authentication information composed of a string of characters, such as letters, numbers, spaces, and other symbols.

Definition of "Physical Safeguards"

Physical measures and related policies and procedures to protect a covered entity's or business associate's relevant electronic information systems, and related facilities and equipment, from natural and environmental hazards and unauthorized intrusion.

Definition of "Relevant Electronic Information System"

An electronic information system that creates, receives, maintains, or transmits ePHI or that otherwise affects the confidentiality, integrity, or availability of ePHI.

This further clarifies the **scope of regulated entities' compliance obligations**, including the obligation of regulated entities to understand the relationship between their various electronic information systems and the confidentiality, integrity, and availability of ePHI.

Definition of "Risk"

The extent to which the confidentiality, integrity, or availability of ePHI is threatened by a potential circumstance or event.

Definitions of "Security or Security Measures"

Encompass all of the administrative, physical, and technical safeguards in or applied to an information system.

Definitions of "Security Incident"

Any of the following:

(1) The **attempted or successful** unauthorized access, use, disclosure, modification, or destruction of information in an information system.

(2) The **attempted or successful** unauthorized interference with system operations in an information system.

Definitions of "Technical Controls"

The technical **mechanisms** contained in the hardware, software, or firmware components of an electronic information system that are primarily implemented and executed by the electronic information system to protect it and the data within the electronic information system.

Definition of "Technical Safeguards"

The technology, technical controls, and related policies and procedures governing the use of the technology that protects and controls access to electronic protected health information.

Definition of "Technology Asset"

The components of an electronic information system, including but not limited to hardware, software, electronic media, information, and data.

This **clarifies which Security Rule requirements apply** to all of the components of electronic information systems as opposed to those that apply only to certain components, and which requirements apply to each particular components and which apply to the entire electronic information system.

Definition of "Threat"

Any circumstance or event with the potential to adversely affect the confidentiality, integrity, or availability of ePHI.

Top 5 Threats Facing the Healthcare Sector

- Social Engineering
- Ransomware
- Loss or Theft of Equipment or Data
- Insider, Accidental or Malicious Data Loss
- Attacks Against Network Connected Medical Devices

https://405d.hhs.gov/cornerstone/hicp

Definition of "User"

A person with authorized access.

Definition of "Vulnerability"

A flaw or weakness in an information system, system security procedures, design, implementation, or technical controls, that could be intentionally exploited or accidentally triggered by a threat.

Definition of "Workstation"

An electronic computing device and electronic media stored in its immediate environment. Workstation includes but is not limited to the following types of devices: a server, desktop computer, laptop computer, virtual device, and a mobile device such as a smart phone or tablet.

Section 164.306—Security Standards: General Rules

- Emphasizes that regulated entities must apply the requirements of the Security Rule to protect all of the ePHI they create, receive, maintain, or transmit.
- A security measure must be implemented such that it protects the security of all ePHI and all information systems that affect the confidentiality, integrity, and availability of ePHI.
- Require each regulated entity to protect against any reasonably anticipated threats or hazards to the confidentiality, integrity, or availability of all ePHI
- Ensure that its workforce complies not only with the Security Rule, but also all administrative, physical, and technical safeguards

Section 164.306(b)—Flexibility of Approach

- Apply reasonable and appropriate security measures to implement the standards and implementation specifications of the Security Rule (in other words, regulated entity may **NOT** determine that implementation itself is unreasonable or inappropriate in some circumstances)
- Require a regulated entity to take into account how effectively its application of a particular security measure to achieve compliance with a standard and its associated implementation specifications would support its resiliency in the face of an event that adversely affects the entity
- "Information system resilience" addresses how well information systems "continue to (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs."
- This new factor would require a regulated entity to consider whether a particular approach to complying with a standard and the associated implementation specifications can help it recover from an emergency or other occurrence, in addition to maintaining operations throughout the event.

Section 164.306(c)—Standards and Implementation Specifications

Removes the distinction between **"addressable" and "required"** implementation specifications. Instead, proposed paragraph (c), would require regulated entities to comply with both the standards and implementation specifications. The Department believes that eliminating the distinction would **make clear to regulated entities** what has always been a requirement—that the Security Rule sets a floor for cybersecurity protections and that its **flexibility is in allowing them to choose the manner in which they meet the standards and implementation specifications, not whether they meet them**.

Section 164.308—Administrative Safeguards

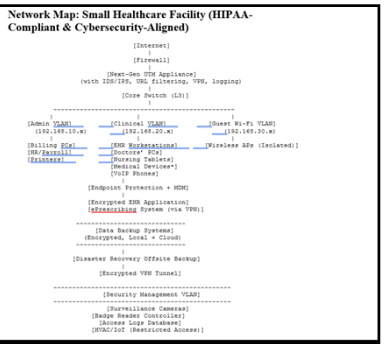
Section 164.308(a)(1)(i)—Standard: Technology Asset Inventory

- Requires a regulated entity to conduct and maintain an accurate and thorough written technology asset inventory and a network map of its electronic information systems (create, receive, maintain, or transmit) and all technology assets that may affect the confidentiality, integrity, or availability of ePHI
- Requires each regulated entity to determine the movement of ePHI through, into, and out of its information systems and to describe such movement in a network map. A regulated entity's network map would reflect where its technology assets are, for example, physically located at the regulated entity's worksite, or accessed through the cloud.
- As another example, a covered entity might determine that ePHI is created, received, maintained, or transmitted by one or more offshore business associates (i.e., persons that are located outside of the U.S.) for such services as claims processing, call center staffing, and technical support, activities that inherently involve ePHI.
- The technology assets used by the business associate to create, receive, maintain, or transmit ePHI are not a part of the covered entity's electronic information system, but do affect the confidentiality, integrity, or availability of ePHI and so would be required to be included in the network map of the covered entity.

Section 164.308(a)(1)(ii)—Standard: Implementation Specifications

A. Inventory
B. Network Map
C. Maintenance

Example of Network Map Criteria



Network Map: Small Healthcare Facility (HIPAA-Compliant & Cybersecurity-Aligned)

[Internet]
|
[Firewall]
|
[Next-Gen UTM Appliance]
(with IDS/IPS, URL Filtering, VPN, logging)
|
[Core Switch (L3)]
|

| | |
[Admin VLAN] [Clinical VLAN] [Guest Wi-Fi VLAN]
(192.168.10.x) (192.168.20.x) (192.168.30.x)
| | |
[Billing PCs] [EHR Workstations] [Wireless APs (Isolated)]
[HR/Payroll] [Doctors' PCs]
[Printers] [Nursing Tablets]
[Medical Devices*]
[VoIP Phones]
|
[Endpoint Protection + MDM]
|
[Encrypted EHR Application]
(ePrescribing System (via VPN))
|

[Data Backup Systems]
(Encrypted, Local + Cloud)

|
[Disaster Recovery Offsite Backup]
|
[Encrypted VPN Tunnel]

[Security Management VLAN]

[Surveillance Cameras]
[Badge Reader Controller]
[Access Logs Database]
[HVAC/IoT (Restricted Access)]

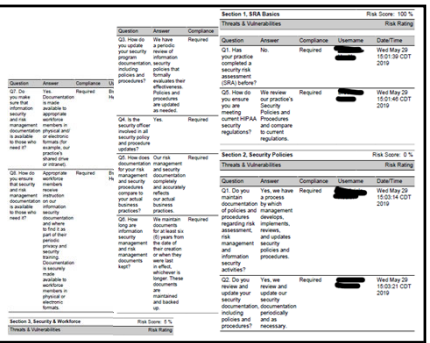
Section 164.308(a)(2)(i)—Standard: Security Risk Analysis

Conduct an accurate and comprehensive written assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained, or transmitted by the covered entity or business associate.

SRA Report outlines vulnerabilities, risk rating, and remediation plans can be documented

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

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



Section 1, SRA Basics — Risk Score: 100 %

Question	Answer	Compliance	Required
Q3. How do you update your security program documentation, including policies and procedures?	We have a periodic review of information security policies that is annually and evaluates their effectiveness. Policies and procedures are updated as needed.		Required
Q4. Is the security officer role and security policy and procedure updates?	Yes.		Required
Q5. How does documentation for your risk management and security procedures reflect your actual business practices?	Our risk management and security documentation completely and accurately reflects our actual business practices.		Required
Q6. How long are information security management documents kept?	We maintain documents for at least six (6) years from the date of creation or when they were last in effect, whichever is longer. These documents are maintained and backed up.		Required

Threats & Vulnerabilities — Risk Rating

Question	Answer	Compliance	Username	Date/Time
Q1. Has your practice completed a security risk assessment (SRA) before?	No.	Required	[redacted]	Wed May 29 15:01:39 CDT 2019
Q5. How do you ensure you are meeting current HIPAA security regulations?	We review our practice's Security Policies and Procedures and compare to current regulations.	Required	[redacted]	Wed May 29 15:01:46 CDT 2019

Section 2, Security Policies — Risk Score: 0 %

Threats & Vulnerabilities — Risk Rating

Question	Answer	Compliance	Username	Date/Time
Q1. Do you maintain documentation of policies and procedures regarding risk assessment, risk management and information security activities?	Yes, we have a process by which management develops, implements, reviews, and updates security policies and procedures.	Required	[redacted]	Wed May 29 15:03:14 CDT 2019
Q2. Do you review and update your security documentation, including policies and procedures?	Yes, we review and update our security documentation periodically and as necessary.	Required	[redacted]	Wed May 29 15:03:21 CDT 2019

Section 3, Security & Workforce — Risk Score: 0 %

Threats & Vulnerabilities — Risk Rating

Section 164.308(a)(2)(ii)—Standard: Implementation Specifications

1. A review of the technology asset inventory
2. Identification of all reasonably anticipated threats
3. Identification of potential vulnerabilities and predisposing conditions
4. An assessment and documentation of the security measures the covered entity or business associate uses
5. A reasonable determination of the likelihood that each threat identified in accordance with paragraph (a)(2)(ii)(A)(2) of this section will exploit the vulnerabilities
6. A reasonable determination of the potential impact of each threat identified
7. An assessment of risk level for each threat identified
8. An assessment of the risks to electronic protected health information posed by entering into or continuing a business associate contract

Section 164.308(a)(2)(ii)—Standard: Implementation Specifications

Review, verify, and update the written assessment on an ongoing basis, but at least once **every 12 months** and **in response to a change** in the covered entity's or business associate's environment or operations that may affect electronic protected health information.

Section 164.308(a)(3)(i)—Standard: Evaluation

Perform a written technical and nontechnical evaluation to determine **whether a change** in the covered entity's or business associate's environment or operations may affect the confidentiality, integrity, or availability of electronic protected health information.

Section 164.308(a)(3)(ii)—Standard: Implementation Specifications

A. Performance
B. Response

Section 164.308(a)(4)(i)—Standard: Patch Management

Implement written policies and procedures for applying patches and updating the configuration(s) of the covered entity's or business associate's relevant electronic information systems.

Section 164.308(a)(4)(ii)—Standard: Implementation Specifications

A. Establish written policies and procedures for identifying, prioritizing, acquiring, installing, evaluating, and verifying the timely installation of patches, updates, and upgrades
B. Maintenance. Review and test written policies and procedures
C. Application. Patch, update, and upgrade the configurations of relevant electronic information systems in accordance with the written policies and procedures – within 15 days
D. Exceptions. Patch not available, would adversely affect security
E. Alternative Measures. Implement reasonable alternatives and compensating controls.
F. Compensation Controls. Implement reasonable and appropriate security measures to address the identified risk in a timely manner until a patch, update, or upgrade that does not adversely affect security.

Section 164.308(a)(5)(i)—Standard: Risk Management

Implement security measures sufficient to reduce risks and vulnerabilities to all electronic protected health information to a reasonable and appropriate level.

Section 164.308(a)(5)(ii)—Standard: Implementation Specfications

A. Planning
B. Maintenance
C. Priorities
D. Implementation

Section 164.308(a)(6)(i)—Standard: Sanction Policy

Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

Section 164.308(a)(6)(ii)—Standard: Implementation Specifications

A. Policy and Procedures
B. Modifications
C. Application

Section 164.308(a)(7)(i)—Standard: Information System Activity Review

Implement written policies and procedures for regularly reviewing records of activity in the covered entity's or business associate's relevant electronic information systems.

Section 164.308(a)(7)(ii)—Standard: Implementation Specifications

A. Policy and Procedures
B. Scope
C. Record Review
D. Record Retention
E. Response
F. Maintenance

Section 164.308(a)(8)(i)—Standard: Assigned Security Responsibility

In writing, identify the security official who is responsible for the development and implementation of the policies and procedures, written or otherwise, and deployment of technical controls required by this subpart for the covered entity or business associate.

Section 164.308(a)(9)(i)—Standard: Workforce Security

Implement written policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information and relevant electronic information systems, and to prevent those workforce members who are not authorized to have access from obtaining access to electronic protected health information and relevant electronic information systems.

Section 164.308(a)(9)(ii)—Standard: Implementation Specifications

A. Authorization and/or supervision
B. Workforce clearance procedure
C. Modification and termination procedures (1 hour)
D. Notification (24 hours)
E. Maintenance

Section 164.308(a)(10)(i)—Standard: Information Access Management

Establish and implement written policies and procedures for authorizing access to electronic protected health information and relevant electronic information systems that are consistent with the applicable requirements of subpart E of this part.

Section 164.308(a)(10)(ii)—Standard: Implementation Specifications

A. Isolating health care clearinghouse functions
B. Access authorization
C. Authentication management
D. Access determination and modification
E. Network segmentation
F. Maintenance

Section 164.308(a)(11)(i)—Standard: Security Awareness Training

Implement security awareness training for all workforce members on protection of electronic protected health information and information systems as necessary and appropriate for the members of the workforce to carry out their assigned function(s)

Section 164.308(a)(11)(ii)—Standard: Implementation Specifications

A. Training
B. Timing (30 days, annually, changes)
C. Ongoing education (reminders)
D. Documentation

Section 164.308(a)(12)(i)—Standard: Security Incident Procedures

Implement written policies and procedures to respond to security incidents.

Section 164.308(a)(12)(ii)—Standard: Implementation Specifications

A. Planning and testing
   1) Establish written security incident response plan(s) and procedures
   2) Implement written procedures for testing and revising security incident response plan(s)
B. Response
   1) Identify and respond to suspected or known security incidents.
   2) Mitigate, to the extent practicable, harmful effects of security incidents
   3) Identify and remediate, to the extent practicable, the root cause(s)
   4) Eradicate the security incidents that are suspected or known
   5) Develop and maintain documentation of investigations, analyses, mitigation, and remediation

Section 164.308(a)(13)(i)—Standard: Contingency Plan

Establish and implement as needed a written contingency plan, consisting of written policies and procedures for responding to an emergency or other occurrence—including but not limited to fire, vandalism, system failure, natural disaster, or security incident—that adversely affects relevant electronic information systems.

Section 164.308(a)(13)(ii)—Standard: Implementation specifications

A. Criticality analysis
B. Data backups
C. Information systems backups
D. Disaster recovery plan
E. Emergency mode operation plan
F. Testing and revision procedures

Section 164.308(a)(14)(i)—Standard: Compliance Audit

Perform and document an audit at least once every 12 months of the covered entity's or business associate's compliance with each standard and implementation specification in this subpart.

Section 164.308(b)(1)(i)—Standard: Business Associate Contracts and Other Arrangements

A. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will comply with this subpart and verifies that the business associate has deployed technical safeguards in accordance with the requirements of § 164.312.
B. A covered entity is not required to obtain such satisfactory assurances or verification from a business associate that is a subcontractor.

Section 164.308(b)(1)(ii)—Standard: Business Associate Contracts and Other Arrangements

A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf **only if the business associate obtains satisfactory assurances**, in accordance with § 164.314(a), **that the subcontractor will comply** with the requirements of this subpart and verifies that the business associate that is a subcontractor has deployed technical safeguards in accordance with the requirements of § 164.312.

Section 164.308(b)(2)(i)—Standard: Implementation Specifications

i. Written contract or other arrangement
ii. Written verification
   A. A written analysis of the business associate's relevant electronic information systems
   B. A written certification that the analysis has been performed and is accurate

Section 164.308(b)(3)—Standard: Delegation to Business Associate

i. A covered entity or business associate may permit a business associate to serve as their designated security official
ii. A covered entity or business associate that delegates actions, activities, or assessments required by this subpart to a business associate remains liable for compliance with all applicable provisions of this subpart.

Section 164.308—Administrative Safeguards

Security Measure Assessment: a regulated entity to take the results of the required tests into consideration when determining whether it is reasonable and appropriate to modify its security measures.

Written policies and procedures can be tested through various methods including, but not limited to: assess how effectively employees follow incident response and security procedures; conducting knowledge assessments after training on policies and procedures; and reviewing system logs and access records to evaluate whether policies and procedures governing access to ePHI are being followed.

Section 164.310 Physical Safeguards

Section 164.310(a)—Standard: Facility Access Controls

Establish and implement written policies and procedures to limit physical access to all of its relevant electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Section 164.310(a)(2)—Standard: Implementation Specifications

i. Contingency operations
ii. Facility security plan
iii. Access management and validation procedures
iv. Physical maintenance records
v. Maintenance

Section 164.310(b)—Standard: Workstation Use

Establish and implement written policies and procedures that govern the use of workstations that access electronic protected health information or the covered entity's or business associate's relevant electronic information systems.

Section 164.310(b)(2)—Standard: Implementation Specifications

i. Policies and procedures
ii. Maintenance.

Section 164.310(c)—Standard: Workstation Security

Implement and modify physical safeguards for all workstations that access electronic protected health information or relevant electronic information systems, to address the written policies and procedures for workstation use required by paragraph (b) of this section and restrict access to authorized users.

Section 164.310(d)—Standard: Technology Asset Controls

Establish and implement written policies and procedures that govern the receipt and removal of technology assets that maintain electronic protected health information into and out of a facility, and the movement of these assets within the facility.

Section 164.310(d)(2)—Standard: Implementation Specifications

i. Disposal
ii. Media sanitization
iii. Maintenance

Section 164.312(a) Technical Safeguards

Section 164.312(a)—Standard: Access Control

Deploy technical controls in relevant electronic information systems to allow access only to users and technology assets that have been granted access rights.

Section 164.312(a)—Standard: Implementation Specifications

i. Unique identification
ii. Administrative and increased access privileges
iii. Emergency access procedure
iv. Automatic logoff
v. Log-in attempts
vi. Network segmentation
vii. Data controls
viii. Maintenance

Section 164.312(b)—Standard: Encryption and Decryption

Deploy technical controls to encrypt and decrypt electronic protected health information using encryption that meets prevailing cryptographic standards.

Section 164.312(b)(2)—Standard: Implementation Specification

Encrypt all electronic protected health information at rest and in transit

Section 164.312(b)(3)—Standard: Exceptions

This paragraph (b)(3) applies only to the electronic protected health information directly affected by one or more of the following exceptions:

i. The technology asset in use does not support encryption
ii. An individual requests pursuant to § 164.524 to receive their electronic protected health information in an unencrypted manner and has been informed of the risks associated with the transmission, receipt, and storage of unencrypted electronic protected health information.
iii. During an emergency or other occurrence that adversely affects the covered entity's or business associate's relevant electronic information systems in which encryption is infeasible
iv. The technology asset in use is a device under section 201(h) of the Food, Drug, and Cosmetic Act, 21 U.S.C. 321(h) that has been authorized for marketing by the Food and Drug Administration

Section 164.312(b)(4)—Standard: Alternative measures

i. Alternative measures. Where an exception at paragraph (b)(3) of this section applies, a covered entity or business associate must document in real-time the existence of an applicable exception and implement reasonable and appropriate compensating controls in accordance with paragraph (b)(4)(ii) of this section.
ii. Compensating controls
   A. The covered entity or business associate must secure such electronic protected health information by implementing reasonable and appropriate compensating controls
   B. The covered entity or business associate shall be presumed to have implemented reasonable and appropriate compensating controls where the covered entity or business associate has deployed the security measures prescribed and as instructed by the authorized label for the device, including any updates or patches
   C. The implementation and effectiveness of compensating controls must be reviewed, documented, and signed by the designated Security Official at least once every 12 months or in response to environmental or operational changes

Section 164.312(b)(5)—Standard: Maintenance

Review and test the effectiveness of the technical controls required by this paragraph (b) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

Section 164.312(c)—Standard: Configuration Management

Establish and deploy technical controls for securing the covered entity's or business associate's relevant electronic information systems and technology assets in its relevant electronic information systems, including workstations, in a consistent manner, and maintain such electronic information systems and technology assets according to the covered entity's or business associate's established secure baselines.

Section 164.312(c)(2)—Standard: Implementation Specifications

i. Anti-malware protection
ii. Software removal
iii. Configuration
iv. Network ports
v. Maintenance

Section 164.312(d)—Standard: Audit trail and System Log Controls

Deploy technology assets and/or technical controls that record and identify activity in the covered entity's or business associate's relevant electronic information systems.

Section 164.312(d)(2)—Standard: Implementation Specifications

i. Monitor and identify
ii. Record
iii. Retain
iv. Scope
   A. ePHI
   B. Relevant electronic information systems and the information
v. Maintenance

Section 164.312(e)—Standard: Integrity

Deploy technical controls to protect electronic protected health information from improper alteration or destruction, both at rest and in transit; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

Section 164.312(e)—Standard: Integrity

Deploy technical controls to protect electronic protected health information from improper alteration or destruction, both at rest and in transit; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

Section 164.312(f)—Standard: Authentication

Deploy technical controls to verify that a person or technology asset seeking access to electronic protected health information and/or the covered entity's or business associate's relevant electronic information systems is the one claimed.

Section 164.312(f)(2)—Standard: Implementation Specifications

i. Information access management policies
ii. Multi-factor authentication
   A. Deploy multi-factor authentication to all technology assets
   B. Deploy multi-factor authentication for any action that would change a user's privileges
iii. Exceptions
   A. The technology asset in use does not support multi-factor authentication, establish and implement a written plan to migrate information to a technology asset that supports multifactor authentication within a reasonable and appropriate period of time.
   B. During an emergency
   C. The technology asset in use is a device under section 201(h) of the Food, Drug, and Cosmetic Act, 21 U.S.C. 321(h) that has been authorized for marketing by the Food and Drug Administration

Section 164.312(f)(2)—Standard: Alternative measures

i. Alternative measures. Where an exception at paragraph (b)(3) of this section applies, a covered entity or business associate must document in real-time the existence of an applicable exception and implement reasonable and appropriate compensating controls in accordance with paragraph (f)(2)(iv)(B) of this section.
ii. Compensating controls
   A. The covered entity or business associate must secure such electronic protected health information by implementing reasonable and appropriate compensating controls
   B. The covered entity or business associate shall be presumed to have implemented reasonable and appropriate compensating controls where the covered entity or business associate has deployed the security measures prescribed and as instructed by the authorized label for the device, including any updates or patches
   C. The implementation and effectiveness of compensating controls must be reviewed, documented, and signed by the designated Security Official at least once every 12 months or in response to environmental or operational changes

Section 164.312(f)(2)—Standard: Maintenance

Review and test the effectiveness of the technical controls required by this paragraph (f) at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

Section 164.312(g)—Standard: Transmission Security

Deploy technical controls to verify that a person or technology asset seeking access to electronic protected health information and/or the covered entity's or business associate's relevant electronic information systems is the one claimed.

Section 164.312(g)—Standard: Transmission Security

Deploy technical controls to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

Section 164.312(h)—Standard: Vulnerability Management

Deploy technical controls in accordance with the covered entity's or business associate's patch management policies and procedures required by § 164.308(a)(4)(ii)(A) to identify and address technical vulnerabilities in the covered entity's or business associate's relevant electronic information systems.

Section 164.312(h)(2)—Standard: Implementation Specifications

i. Vulnerability scanning
   A. Conduct automated vulnerability scans to identify technical vulnerabilities at least once every six months
   B. Review and test the effectiveness of the technology asset(s) that conducts the automated vulnerability scans at least once every 12 months
ii. Monitoring
iii. Penetration Testing
   A. A qualified person is a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods
   B. Penetration testing must be performed at least once every 12 months
iv. Patch and update installation

Section 164.312(i)—Standard: Data Backup and Recovery

Deploy technical controls to create and maintain exact retrievable copies of electronic protected health information.

Section 164.312(i)(2)—Standard: Implementation Specifications

i. Data backup
ii. Monitor and identify
iii. Record
iv. Testing

Section 164.312(f)—Standard: Information Systems Backup and Recovery

Deploy technical controls to create and maintain backups of relevant electronic information systems; and review and test the effectiveness of such technical controls at least once every six months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

Section 164.314(a)(1)—Standard: Business Associate Contracts or Other Arrangements

The contract or other arrangement required by § 164.308(b)(2) must meet the requirements of paragraph (a)(2)(i), (ii), or (iii) of this section, as applicable.

Section 164.314(a)(2)—Standard: Implementation Specifications

i. Business associate contracts
   A. Comply with the applicable requirements of this subpart
   B. Ensure that any subcontractors on behalf of the business associate agree to comply with the applicable requirements of this subpart
   C. Report to the covered entity any security incident
   D. Report to the covered entity activation of its contingency plan
ii. Other arrangements
iii. Business associate contracts with subcontractors

Section 164.314(b)(1)—Standard: Requirements for Group Health Plans.

Ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information.

Section 164.314(b)(2)—Standard: Implementation Specifications

i. Safeguard implementation
ii. Separation
iii. Agents
iv. Security incident awareness
v. Contingency plan activation

Section 164.316 Documentation Requirements

The contract or other arrangement required by § 164.308(b)(2) must meet the requirements of paragraph (a)(2)(i), (ii), or (iii) of this section, as applicable.

Section 164.316(a)—Standard: Documentation Requirements

A covered entity or business associate must do all of the following in written form, which may be electronic, taking into consideration the factors in § 164.306(b)

Section 164.316(b)(1)—Standard: Implementation Specifications

1) Time limit
2) Availability
3) Updates

The proposed effective date of a final rule would be 60 days after publication

Regulated entities would have until the "compliance date" to establish and implement policies, procedures, and practices to achieve compliance with any new or modified standards.

Where do I go from here?

HICP's 10 Mitigating Practices

1. Email Protection Systems
2. Endpoint Protection Systems
3. Identity and Access Management
4. Data Protection and Loss Prevention
5. IT Asset Management
6. Network Management
7. Vulnerability Management
8. Security Operations Center & Incident Response
9. Network Connected Medical Device Security
10. Cybersecurity Oversight and Governance

Email Protection Systems

The two most common phishing methods occur by email access:

1) Credential theft is where attackers leverage emails to conduct **credential harvesting attacks** on the organization.
2) Malware dropper attacks are used when attackers **deliver malware through emails**, which can compromise endpoints.

An organization's cybersecurity practices must address these two attack vectors.

Because both attack types leverage email, **email systems should be the focus for additional security controls**.

Endpoint Protection Systems

An organization's endpoints must be protected. Endpoints include **desktops, laptops, mobile devices, and other connected hardware devices** (e.g., printers, medical equipment).

Because technology is highly mobile, computers are often connected to and disconnected from an organization's network.

Identity and Access Management

Health care organizations of all sizes need to **clearly identify all users and maintain audit trails** that monitor each user's access to data, applications, systems, and endpoints.

Just as you may use a name badge to identify yourself in the physical work environment, cybersecurity access management practices can help ensure that **users are properly identified** in the digital environment, as well.

Data Protection and Loss Prevention

A security breach is the loss or exposure of sensitive data, including information relevant to the organization's business and patient PHI.

Impacts to the organization can be profound if data are corrupted, lost, or stolen.

IT Asset Management

Organizations manage IT assets using processes referred to collectively as IT asset management (ITAM).

ITAM is critical to ensuring that the appropriate **cyber hygiene controls are maintained across all assets** in your organization

Network Management

Computers communicate with other computers through networks.

These networks are connected wirelessly or via wired connections (e.g., network cables), and networks must be established before systems can interoperate.

Networks that are established in an insecure manner increase an organization's exposure to cyberattacks.

Vulnerability Management

Organizations manage IT assets using processes referred to collectively as IT asset management (ITAM).

ITAM is critical to ensuring that the appropriate **cyber hygiene controls are maintained across all assets** in your organization.

Security Operations Center & Incident Response

Incident response is the ability to discover cyberattacks on the network and prevent them from causing data breach or loss.

Incident response is often referred to as the standard "blocking and tackling" of information security. Many types of security incidents occur on a regular basis across organizations of all sizes.

Two common security incidents that affect organizations of all sizes are:

1) the installation and detection of malware, and
2) phishing attacks that include malicious payloads (via attachments and links).

Network Connected Medical Device Security

Medical devices are essential to diagnostic, therapeutic and treatment practices. These devices deliver significant benefits and are successful in the treatment of many diseases. As with all technologies, medical device benefits are accompanied by cybersecurity challenges.

Cybersecurity vulnerabilities are introduced when medical devices are connected to a network or computer to process required updates, therefore in order to protect patients it is important to protect these devices.

Medical devices are a specialized type of **Internet of Things (IoT)** device and rather than recreating cybersecurity practices for them, healthcare organizations are encouraged to **extend the relevant cybersecurity practices** from each of the other prescriptions, and implement them appropriately for medical device management.

Cybersecurity Oversight and Governance

Establishing and implementing cybersecurity **policies, procedures, and processes** is one of the most effective means of preventing cyberattacks.

They set expectations and foster a consistent adoption of behaviors by your workforce.

With clearly articulated cybersecurity policies, your employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.

Basic EHRs versus Certified EHRs

What's the bottom line?

We comply or don't comply to the rules through our technology's capabilities…

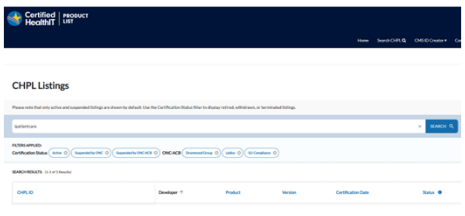
How do we achieve compliance to this rule?

Use a certified EHR System that provides the API, Patient Portal, and interoperability capabilities needed…

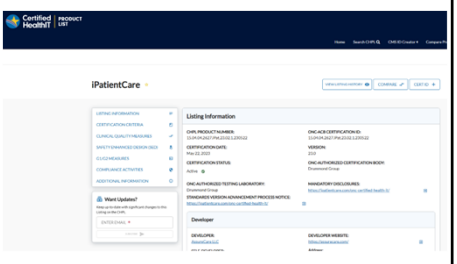
https://www.healthit.gov/curesrule/resources/information-blocking-faqs

Search the ONC website here:

https://chpl.healthit.gov/#/search



The EHR you are searching will show up here if it is certified:



A Patient Portal allows patients access to their EHI

https://www.bpaehr.com/

Questions?

Info@ClinicArmor.com

Thank you!