COMPLIANCE OVERVIEW

HIPAA Security Rule

The HIPAA Security Rule establishes **national standards for securing individuals' electronic protected health information (ePHI).** These standards require covered entities (and their business associates) to analyze the risks and vulnerabilities of the confidentiality, integrity and availability of their ePHI. The risk assessment process helps covered entities and business associates implement reasonable and appropriate administrative, physical and technical safeguards to protect their ePHI.

The Security Rule only applies to ePHI—it does not apply to PHI that is in paper or written form and it also does not apply to electronic personal information that is not PHI.

Covered entities and business associates should periodically revisit their risk assessments and make appropriate updates to their ePHI safeguards. According to the Department of Health and Human Services (HHS), compliance with the HIPAA Security Rule is not a one-time project, but rather an ongoing process that involves new security challenges as organizations and technologies change.

LINKS AND RESOURCES

- HHS' website includes a brief summary of the HIPAA Security Rule and links to the official regulation text.
- HHS has provided the following resources:
  - Risk Analysis Guidance
  - Cyber Security Guidance
  - Security Risk Assessment Tool

Affected Entities

- The HIPAA Security Rule applies to covered entities and business associates.
- A covered entity is a health plan, a health care clearinghouse or a health care provider that conducts certain transactions electronically.
- In general, a business associate is an entity that performs a function, activity or specific service for a covered entity that involves PHI.

Risk Assessment

- Covered entities and business associates must analyze the potential risks and vulnerabilities of their ePHI.
- Based on this analysis, covered entities and business associates must implement reasonable and appropriate safeguards.
- Risk assessment is an ongoing process.

COMPLIANCE OVERVIEW

Affected Entities

The HIPAA Security Rule directly regulates these covered entities:

- ☑ Health plans;
- ☑ Health care clearinghouses; and
- ☑ Health care providers that conduct certain transactions electronically.

Business Associates

Business associates also must comply with many provisions of the Security Rule. For additional protection, covered entities and business associates must enter into agreements requiring them to comply with the HIPAA Privacy and Security Rules.

> ***Who is a business associate?***
> In general, a business associate is an entity that performs a function, activity or specific service for a covered entity that involves creating, receiving, maintaining or transmitting PHI.

If a business associate delegates any of its functions to a subcontractor that creates, receives, maintains or transmits ePHI on behalf of the business associate, the business associate must enter into a written contract with the subcontractor to ensure that the subcontractor will agree to comply with the HIPAA Privacy and Security Rules.

Plan Sponsors

The Security Rule indirectly regulates employers as plan sponsors. In general, sponsors of self-insured and fully insured group health plans should conduct risk assessments and implement appropriate safeguards to protect their ePHI. Unlike the Privacy Rule, the Security Rule does not contain a special exception for fully insured plans that do not have access to PHI for plan administration purposes. However, fully insured health plans that do not handle PHI will have fewer obligations under the Security Rule due to their "hands off" approach to PHI.

Protected Information

The HIPAA Security Rule governs ePHI. PHI is individually identifiable health information (in oral, written or electronic form) that is created or received for a covered entity and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.

Electronic PHI is PHI that is transmitted by, or maintained in, electronic media. For example, this includes PHI in computers, devices that are used with computers, (such as disks and drives) and smartphones. It also includes PHI that is sent via email or in any manner using the Internet. Written or oral communications are not ePHI, and, thus, are not subject to the Security Rule. However, all types of PHI (written, oral and electronic) are subject to the Privacy Rule's use and disclosure rules.

The Security Rule's requirements apply even when the ePHI is located on a device that is not owned by the covered entity (for example, an employee's smartphone) or is accessed outside of the covered entity's physical location (for example, on a home computer or on a laptop outside of work). HHS has cautioned that covered entities should be extremely careful about allowing off-site use of, or access to, ePHI due to security risks involved.

Security Requirements

The HIPAA Security Rule requires that covered entities do the following:

- ☑ Ensure the confidentiality, integrity and availability of all ePHI it creates, receives, maintains or transmits;
- ☑ Protect against any reasonably anticipated threats or hazards to the security or integrity of this information;
- ☑ Protect against reasonably anticipated use or disclosure of this information that is not permitted or required under the HIPAA Privacy Rule; and
- ☑ Ensure its workforce complies with the procedures implemented to comply with the HIPAA Security Rule.

Risk Assessment

According to HHS, performing a risk analysis is a crucial first step in identifying and implementing reasonable and appropriate security standards. A risk assessment helps an organization establish appropriate administrative, physical and technical safeguards for its ePHI. It directs what reasonable steps a covered entity or business associate should take to protect the ePHI it creates, transmits, receives or maintains. Risk assessment is also an **ongoing process**. Covered entities and business associates should periodically revisit their risk assessments and make appropriate updates to their ePHI safeguards.

Security Standards

The security standards are divided into the following three categories:

Administrative Safeguards	Physical Safeguards	Technical Safeguards
Establish standards and specifications for the health information security program. Examples: • Staff training to ensure knowledge of and compliance with policies and procedures • Information access management to limit access to ePHI	Control physical access to the office and computer systems. Examples: • Facility access controls, such as locks and alarms, to ensure only authorized personnel have access to facilities that house systems and data • Workstation security measures, such as cable locks and computer	Include hardware, software and other technology that limits access to ePHI. Examples: • Access controls to restrict access to ePHI to authorized personnel only • Audit controls to monitor activity on systems containing ePHI

Administrative Safeguards	Physical Safeguards	Technical Safeguards
• Contingency plan to respond to emergencies or to restore lost data	monitor privacy filters, to guard against theft and restrict access to authorized users • Workstation use policies to ensure proper access to and use of workstations	• Integrity controls to prevent improper ePHI alteration or destruction • Transmission security measures to protect ePHI when transmitted over an electronic network

Implementation Specifications

Each type of safeguard—administrative, physical and technical—has certain standards and implementation specifications associated with it. The Security Rule allows covered entities some flexibility in determining how to implement the standards and implementation specifications, including choosing which technology it will employ in order to achieve the required security standards.

In deciding how to implement security measures, a covered entity is permitted to consider:

- Its size, complexity and capabilities;
- Its technical infrastructure, hardware and software security capabilities;
- The costs of security measures; and
- The probability and criticality of potential risks to health information.

However, HHS has stated that cost alone is not a justification for failing to implement a procedure.

In an effort to provide covered entities with additional flexibility with respect to complying with the Security Rule, the regulations set forth two categories of implementation specifications: **"required" and "addressable."**

REQUIRED	When an implementation specification is "required," the covered entity must meet the implementation specifications. The following are examples of "required" implementation specifications: • Entering into business associate contracts; • Conducting a risk analysis; and • Controlling access to ePHI through the of use unique user identification.
ADDRESSABLE	"Addressable" implementation specifications are **not optional**. Rather, a covered entity is provided more flexibility in determining how it will comply with an "addressable" implementation specification. If an implementation specification is "addressable," a covered entity is required to do one of the following:

- If an "addressable" implementation specification is reasonable and appropriate, then the covered entity must implement it.
- If an "addressable" implementation specification is not appropriate and/or reasonable, then the covered entity must implement an alternate measure that accomplishes the same result, if reasonable and appropriate.
- If an "addressable" implementation specification is not applicable to the situation and that standard can be met without implementation of an alternate measure in place of the "addressable" implementation specification, the covered entity can choose not to implement the "addressable" implementation specification.

In all cases, a covered entity should document the reasons for each of its decisions and the procedures implemented to comply with the Security Rule.

Policies and Procedures

Covered entities are required to implement reasonable and appropriate policies and procedures to comply with the HIPAA Security Rule's standards and implementation specifications. These policies and procedures must be documented in written form, which may be electronic.

A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of ePHI. Documentation supporting its security policies must be retained **for at least six years** from the date of its creation or the date when it was last in effect, whichever is later.

Enforcement

HHS' Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Security Rule. OCR has increased its enforcement of the HIPAA Privacy and Security Rules in recent years, with some costly outcomes for covered entities. OCR enforces HIPAA's Privacy and Security Rules by investigating complaints that are filed with it, conducting compliance reviews of covered entities and business associates and performing education and outreach to promote compliance with the Rules' requirements. OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA.

An OCR investigation may trigger civil penalties for a covered entity or business associate. The penalty amounts vary based on the type of violation and are annually adjusted for inflation. Also, penalties may not apply if the violation is corrected within 30 days of when the person knows, or should have known, of the violation.

These civil penalty amounts are subject to annual inflation-related increases. The penalty amounts that apply to civil penalties that are assessed on or after March 17, 2020 (and relate to violations occurring after Nov. 2, 2015) are as follows:

Type of Violation	Minimum Penalty/Violation	Maximum Penalty/Violation
Did not know about violation	$127	$63,973
Violation due to reasonable cause	$1,280	
Corrected violation caused by willful neglect	$12,794	
Violation caused by willful neglect, not corrected	$63,973	$1,919,173

The possible **criminal penalties** that may be assessed for violations of the HIPAA Privacy and Security Rules are a fine of $50,000 and one year in prison for knowing violations, a fine of $100,000 and five years in prison for violations committed under false pretenses, and a fine of $250,000 and 10 years in prison for offenses committed for commercial or personal gain.

HIPAA SECURITY RULE SAFEGUARDS

STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS R= REQUIRED A=ADDRESSABLE
ADMINISTRATIVE SAFEGUARDS		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure (A)
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Functions (R)
		Access Authorization (A)
		Access Establishment and Modification (A)

HIPAA SECURITY RULE SAFEGUARDS

STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS R= REQUIRED A=ADDRESSABLE
Security Awareness Management	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedures (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts & Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement (R)
PHYSICAL SAFEGUARDS		
Facilities Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Reuse (R)
		Accountability (A)
		Data Backup and Storage (A)

HIPAA SECURITY RULE SAFEGUARDS

STANDARDS	SECTIONS	IMPLEMENTATION SPECIFICATIONS R= REQUIRED A=ADDRESSABLE
TECHNICAL SAFEGUARDS		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic PHI (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)