Regulations and Telehealth

by Capella Healthcare

WHAT'S COVERED

In this lesson, you will learn about different telehealth regulations. Specifically, this lesson will cover:

1. HIPAA
   a. Privacy Rule
   b. Security Rule
   c. Breach Notification Rule
   d. Other Rules
2. Confidentiality of Substance Abuse Treatment Disorders

1. HIPAA

HCPs will need to understand and apply compliance measures with regulations while preparing and engaging in telehealth arrangements. A key piece of legislation is HIPAA, which stands for the Health Insurance Portability and Accountability Act (CFR 45, Part 164). It is legislation or law that defines rules for managing privacy and security of covered information (also called protected health information or PHI), grants individuals access to their own medical records, and supports the rights of individuals to authorize viewing (or disclosure) of their own medical records outside of treatment/payment/healthcare operations.

HIPAA was enacted and signed into law in 1996 to ensure national standards for healthcare transactions. Several updates occurred over the last 24 years to include:

- Meaningful Use: Incentives for medical providers that began making medical records electronic and adopting health information technology (HIT) to improve healthcare (CMS).
- Administrative Simplification Rules: Rules to reduce paperwork and create standards in healthcare transactions and privacy/security. There are five rules under Administrative Simplification. The rules include:
  - Privacy
  - Security
  - Breach Notification
  - Transactions and Code Sets
  - National Provider and Employer Identification Standards

Key requirements of HIPAA as it relates to telehealth are:

- Obtaining authorization to treat
- Explaining privacy practices and providing practices in the written or electronic form to the patient
- Employing physical, technical, and administrative safeguards
- Ensuring the right of access to medical records
- Ensuring other HCPs in the organization comply with rules

1a. Privacy Rule

The privacy rule determines standards for PHI protections and uses. It covers all forms of PHI, whether spoken, written, or electronic. This rule defines privacy practices, right of access, and uses and disclosures of PHI. An exception to an individual's right of access is if the provider is a correctional institution. Other exceptions include healthcare treatment, payment, and operations (TPO) with signed consent to treat form (HHS, 2020).
The privacy rule applies to all forms of protected health information (PHI) in any form, whether spoken, written, or stored in systems. The rule is concerned with the right of access, consent to treat, disclosure, and correction of protected health. PHI comprises 18 identifiers. The elements are:

- Name
- Address (all geographic subdivisions smaller than a state, including street address, city, county, and zip code)
- All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death, and exact age if over 89)
- Telephone number
- Fax number
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image (photographic images are not limited to images of the face)
- Any other characteristic that could uniquely identify the individual

1b. Security Rule

The security rule covers ePHI protections and confidentiality/integrity/availability safeguards. Refer to the matrix below for specific requirements under the rule.
The security rule applies to electronic forms of PHI stored in systems. The rule identifies requirements for administrative, physical, and technical safeguards (countermeasures to ensure the confidentiality, integrity, and availability of PHI).

Key requirements for security countermeasures include:

- Technical Safeguards
  - Ensure secure connection for telehealth engagements.
  - Ensure complex passwords.
- Administrative Safeguards
  - Ensure security and privacy training requirements are met for staff.
  - Ensure policies are documented and communicated to staff.
- Physical Safeguards
  - Ensure physical security of systems and physical records dictated from engagements.
    - Workstation and monitor positioning
    - Coversheets for printed PII and PHI
    - Secure location to store computer systems when no longer needed
    - Limits on unauthorized individuals in treatment or meeting areas

Below is the Security Standards Matrix, which can be found as Appendix A of the HIPAA Security Rule.

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)

		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
Technical Safeguards (see §164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

1c. Breach Notification Rule

The HIPAA breach notification rule established standards for breaches of unsecured PHI. Per the ONC Breach Notification Playbook (2020), the HCP (and respective provider) should address the security of ePHI and PHI, devices, and networks to manage and reduce the chance of breaches occurring.
For secured PHI, an unauthorized person cannot use, read, or decipher any PHI that he/she obtains if your practice engages in the following procedures:

- Encrypts the information
- Clears, purges, or destroys media (e.g., data storage devices, film, laptops) that stored or recorded PHI
- Shreds or otherwise destroys paper PHI (These operations must meet applicable federal standards.)

For unsecured PHI, an unauthorized person may use, read, and decipher PHI that he/she obtains if your practice engages in the following procedures:

- PHI is not encrypted or destroyed per federal standards prior to breach.
- Encryption and passwords are easily breakable.

The Breach Notification Rule establishes requirements for reporting unauthorized disclosures (breaches) of PHI in all forms. A covered entity will need to notify impacted individuals that their information was disclosed. Unauthorized disclosure can occur in many forms.

A condition that may constitute a breach occurs if an individual who is not authorized hears an interaction with a patient while the provider (on their end) is engaged in a patient encounter. The same is true if the covered entity does not encrypt the connection for the telehealth engagement, uses an open wireless access point, or uses an insecure application that stores PHI. A risk assessment is needed to determine whether an event is a breach of PHI under HIPAA (ONC, 2020).

HINT

A provision for patients: If the same occurs on the patient's end (use of insecure device or browser), the incident is not considered a breach. Exceptions will be made on a case-by-case basis. Patients should be trained on security measures to protect their information.

1d. Other Rules

The rules that are indirectly related to telehealth but should be briefly discussed for the roles in healthcare treatment, payment, and operations (TPO) are:

- The Employer Identification Standard: Requires employer identification numbers on electronic transactions.
- The National Provider Identification Standards: Requires covered entities to provide their identifier for medical transactions and sharing of medical records for TPO under HIPAA.
- Transactions and Code Set Standards: Establishes coding standards for medical billing and de-identification for statistics/aggregate reporting.

2. Confidentiality of Substance Abuse Treatment Disorders

When considering privacy and security of health information, super-sensitive information such as data on pregnancy, AIDS/HIV, some components of behavioral health, and/or substance abuse treatment (informally referred to as "Super PHI") may require additional protections. The HIPAA Privacy Rule requires enhanced protections of this information category (HHS).

A covered entity may also have requirements under the Confidentiality of Substance Abuse Disorders, also known as 42 CFR Part 2. While HIPAA is governed by the Department of Health and Human Services (HHS), 42 CFR Part 2 is governed by the Substance Abuse and Mental Health Administration (SAMHSA). As it relates to telehealth engagements, environment and system securities are similar to the requirements under HIPAA Privacy and Security Rules. This includes authorization to treat, and physical, administrative, and technical safeguards.

For more information, access the following links:

- Substance Abuse Confidentiality Regulations
- The Confidentiality Of Alcohol And Drug Abuse Patient Records Regulation And The Hipaa Privacy Rule

Authored by Cindy Ebner, MSN, RN, CPHRM, FASHRM and Tamika K. Williams, MSIT.CS, CISM, CISSP, CAP, SSCP, HCISPP, COBIT 5 Foundation/Implementation

Support

If you are struggling with a concept or terminology in the course, you may contact **TelehealthSupport@capella.edu** for assistance.

If you are having technical issues, please contact **learningcoach@sophia.org**.