HIPAA Basics, EverFi Training Module

Highlights for Advisors

HIPAA Sets a National Standard

To ensure both the proper access to and confidentiality of medical records, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA is a federal law that establishes the rules for managing medical information throughout the United States. Although states may adopt stricter confidentiality rules, HIPAA sets the minimum standards and protections for medical privacy.

This course focuses on HIPAA rules affecting the privacy and security of health care information.

In addition to protecting privacy, HIPAA also:

- increases portability and limits pre-existing condition exclusions in health insurance
- simplifies claims management by standardizing code sets and transactions
- requires staff be trained on HIPAA policies and procedures

In 2009, HIPAA was amended by the Health Information Technology for Economic and Clinical Health Act (HITECH). These amendments, which became effective in 2013, add strict new penalties – including the possibility of personal criminal liability – and make compliance with HIPAA's privacy and security standards even more important.

Business Associates

HIPAA also covers "business associates" who have access to health care information from covered entities.

Business Associates

"Business associates" are individuals and organizations (including contractors and other non-staff) who perform certain services and activities, such as:

- claims processing and third-party billing
- administrative, management, and professional consulting
- data transmission, storage, and aggregation (including web-hosting)

Originally, HIPAA only required business associates to sign written agreements promising to keep medical information confidential. However, because of the HITECH amendments, business associates are now directly covered by HIPAA and subject to its privacy and security rules.

As a result, many businesses that aren't in the medical field must now comply with HIPAA. For example, if a truck containing medical records is stolen, the delivery company may be required to notify the affected individuals or face HIPAA penalties.

HIPAA Privacy Rule

The HIPAA "Privacy Rule" requires the confidentiality of medical information.

Issued by the US Department of Health & Human Services (HHS), the official name of the regulation is "The Standards for Privacy of Individually Identifiable Health Information" [45 CFR Part 160 and Subparts A and E of Part 164].

The HIPAA Privacy Rule:

- protects individually identifiable health information
- requires organizations to establish safeguards to ensure medical privacy
- restricts the use and disclosure of medical information
- gives patients the right to access and control their medical records

The Privacy Rule protects health information from the time a record is created (or the information is revealed) to the time it's destroyed. Generally, covered entities and business associates may not use or release an individual's medical information unless the Privacy Rule expressly permits it, or the individual authorizes it. And when medical information may be shared, the Privacy Rule strictly limits the amount of information that may be provided.

Protected Health Information (PHI)

Because HIPAA is designed to protect personal privacy, the Privacy Rule applies to any "individually identifiable health information."

Thus, any information or record, in any form or media (including electronic, paper, or oral), about an individual's mental or physical health, condition, or treatment (whether past, present, or future), should be considered Protected Health Information (PHI).

According to HIPAA, medical records and data are PHI when they contain "individual identifiers" such as:

- names

- contact information (street or email address, telephone or fax number)
- dates directly relating to an individual (birth or death, admission or discharge)
- geographic subdivisions smaller than a state (county, city, zip code)
- account numbers (Social Security, medical record, insurance)
- biometric identifiers (fingerprint, retinal scan, full-face photograph)
- other unique identifiers (certificate or license number, vehicle license plate, Web URL, IP address)

By contrast, if information doesn't relate to specific people (such as a hospital's annual occupancy rate), it probably isn't PHI.

Individual Rights Under HIPAA

HIPAA also gives individuals control over their own PHI, including the right to:

- access their PHI
- obtain copies of their PHI (including electronic records) within 30 days
- request amendments to correct or complete their records
- request confidential communications
- obtain an accounting of who used or received their PHI
- impose restrictions on disclosure of their PHI under certain conditions
- opt out of fundraising communications
- revoke previous authorizations
- file complaints

HIPAA requires organizations to establish policies to timely respond to individuals seeking to exercise their rights.

Limited Use and Disclosure

Even when PHI may be shared, the Privacy Rule strictly limits the amount of information that may be given. In most situations, disclosure must be restricted to the minimum necessary that is needed to accomplish the task. This is called the HIPAA "minimum necessary" rule.

This means you should not access, acquire, examine, talk about, or share PHI unless required by your assigned duties. And, if you're authorized to disclose PHI, remember to restrict the disclosure to only what is authorized and necessary for the recipients to do their jobs.

It is not necessary to limit disclosures:

- to health care providers when PHI is requested for treatment or evaluation
- to the individual who is the subject of the information
- if authorized by the individual
- during government investigations or if otherwise required by law
- to comply with other HIPAA rules

HIPAA Authorized Disclosures

Although HIPAA ordinarily restricts sharing health information, it requires organizations to disclose PHI in two situations:

- when an individual (or their personal representative) requests their own information
- to respond to investigations by the Department of Health & Human Services

Additionally, HIPAA permits organizations to disclose PHI when:

- needed for the public interest
- used specifically for "treatment, payment, and health care operations" (TPO)
- the disclosure is "incidental" to other appropriate use
- going to another person or entity authorized by the individual

Public Interest Disclosures

An organization may disclose PHI in the public interest, including:

- when required by law (to report suspected abuse, neglect, or domestic violence)
- to support public health or health oversight activities (to report communicable diseases)
- to comply with orders, subpoenas, and warrants in judicial and administrative proceedings

- to help law enforcement identify a missing person or fugitive
- to facilitate the donation or transplantation of cadaveric organs, eyes, and tissue
- to funeral directors, coroners, or medical examiners to identify a deceased person or the cause of death
- when used for research projects or clinical trials if certain minimum safeguards (including a privacy board) are satisfied
- to comply with workers' compensation laws

Thus, HIPAA allows for some PHI to be disclosed without a patient's authorization.

Your Security Responsibilities

HIPAA requires organizations to protect PHI (and E-PHI) from the time data is collected until it is destroyed. Staff are responsible for taking reasonable measures to protect information from unauthorized disclosure. For example you should practice:

• Verbal awareness: Speak quietly and avoid using patients' names when discussing health care in public areas such as waiting rooms, hallways, and elevators; try to use a private office when answering patients' questions or discuss PHI on the telephone; and avoid overhearing when other staff discuss PHI at work.

• Physical awareness: Don't permit health care information to be seen by others (don't read files on the bus, leave paperwork on a desk, or visible to others on a screen), and don't leave it unattended (in a copy machine, restaurant, or car).

• Transmission awareness: Verify addresses and fax numbers before sending documents; when possible, use secure (encrypted) systems to send E-PHI rather than ordinary Internet email; and don't download unencrypted E-PHI outside the system to public or remote computers or copy it to media (disks, CDs) or devices (PDAs, thumb drives).

• Destruction awareness: Ensure that PHI is no longer accessible when it is discarded, such as by shredding paper records or securely erasing E-PHI from media before it is recycled; don't simply throw PHI or E-PHI in the trash.

Your organization should provide specific information and updates regarding the applicable security procedures and your responsibility to protect (backup) or destroy (shred) PHI or E-PHI. Security and protecting health care information is an ongoing project; expect periodic security reminders.