HIPAA Training

INTRODUCTION

Efficient quality patient care relies on the sharing of patient information. Current technology and its natural progression allows for the quick access of this patient information, making it increasingly more difficult to protect the privacy of patient health information.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. HIPAA was established to regulate the exchange of patient information and to maintain the security and privacy of that information. The Department of Health and Human Services (HHS) published two rules under HIPAA, the Privacy Rule and the Security Rule.

COMPLIANCE

HIPAA states that all covered entities must comply with HIPAA standards. A covered entity is:

- Healthcare provider who transmits data electronically (for example, doctors, hospitals, dentists, nursing homes, pharmacies, etc.,)
- Any person or organization that furnishes, bills, or is paid for healthcare services in the normal course of business, and electronically transmits and stores that healthcare information. A healthcare provider can also include a person or organization that engages a third party to process, transmit, and store their claims electronically.
- Health plans
- Healthcare clearinghouses

PHI DEFINED

PHI (protected health information) is individually identifiable health information that can be traced to a patient. PHI details the patient status, treatment, and payment information that is managed by a covered entity.

Individually identifiable health information is any information that would clearly identify an individual or could potentially identify an individual even if the individual is not named.

A covered entity in the role of an employer that possesses individually identifiable health information of an employee in the form of education or employment records is not considered to possess PHI. Examples of PHI include, but are not limited to, the following:

- Patient's name
- Patient's address
- Any elements of dates that are directly related to an individual, including birth date, admission date, discharge date, death date
- Telephone numbers, fax numbers, or email addresses
- Social Security Numbers, medical record numbers, or account numbers
- The individual's URL or ISP address
- Health plan beneficiary numbers (insurance numbers)
- Certificate/license numbers
- Vehicle identifiers, serial numbers, or license plate numbers
- Device identifiers and serial numbers
- Biometric identifiers, including finger and voice prints
- Full-face photographs or any comparable images
- Any other unique identifying number, characteristic, or code

PHI USE AND DISCLOSURE

The HIPAA Privacy Rule permits the use and disclosure of PHI under the following situations:

- For treatment
- For payment
- For healthcare purposes
- Individual authorization
- For legal requirements

The HIPAA Privacy Rule protects the privacy of patient information. An employee of a covered entity who manages patient information must be in compliance with the HIPAA Privacy Rule. Failure to do so could result in punitive measures and fines for all individuals involved. PHI can be used without verbal or signed consent for the purpose of necessary treatment, payment, or healthcare operations.

The HIPAA Privacy Rule requires covered entities to practice limiting the use of PHI to the minimum necessary to accomplish the intended purpose.

- The minimum necessary standard does NOT apply to the following:
  - Disclosures to or requests by a healthcare provider for treatment purposes
  - Disclosures to the individual who is the subject of the information (i.e. patient)
  - Uses or disclosures authorized by the patient
  - Uses or disclosures required for compliance with HIPAA Rules
  - Disclosures to Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes
  - Uses or disclosures that are required by other law

The Minimum Necessary Rule mandates that only the information needed to perform the task be provided. Authorization must be given by the patient to the relevant healthcare organization before the use of patient materials in marketing and advertising. Every healthcare organization should have written policies and procedures regarding the use of PHI. Healthcare providers need to be aware of their own organization's policies and procedures.

THE PRIVACY RULE

The Privacy Rule under HIPAA protects the privacy of all PHI.

- In general, HIPAA Privacy Rule requirements:
  - Apply to most healthcare providers
  - Set a federal floor for protecting individually identifiable health information across all mediums (electronic, paper, or verbal)
  - Limit how covered entities may use or disclose individually identifiable health information received or created
  - Give individuals rights with respect to their PHI, including a right to examine and obtain a copy of information in their medical records, and the right to ask covered entities to amend their medical record if information is inaccurate or incomplete
  - Impose administrative requirements for covered entities, and establish civil penalties
- Under the HIPAA Privacy Rule:
  - All patients MUST receive a healthcare organization's Notice of Privacy Practices.
  - Patients may give a verbal authorization to provide PHI to family members and friends.
  - Patients are notified of their rights to complain about an organization's compliance with the Privacy Rule.
  - Patients have the right to access and amend their own PHI.

THE SECURITY RULE

The Security Rule imposes a set of national security standards for protecting PHI in electronic form. Violations of PHI privacy under HIPAA could result in imprisonment and fines enforced by the Office of Civil Rights and the Department of Justice. Examples of electronic storage mediums used for transmission of data could include, but not be limited to:

- Internet
- Extranet
- Intranet
- Leased lines
- Dial-up lines
- Private networks
- Physical movement of removable/transportable electronic storage media

The electronic health record is another means of storing PHI in electronic form. The Security Rule requires covered entities to establish security measures to protect patient privacy and to comply with HIPAA regulations.

PROTECTING PHI

There are many ways that PHI can be compromised. Here are a few examples:

- Face-to-face conversations
- Telephone conversations
- Unprotected computers and facsimile
- Mobile devices (texting/email)
- Unsecured storage of PHI (unsecured networks, unlocked file cabinets)
- Improper trash disposal of PHI
- Unauthorized access to PHI

PHI ACCESS AND DISCLOSURE

Patients have the right to access their own PHI. Once a request for access has been made, the covered entity has 30 days to respond to that request. An exception to this would be psychotherapy notes and information pertaining to criminal, civil, or administrative action.

Patients have the right to amend their own PHI. To submit changes to PHI, a request in writing by the patient may be required by the organization as well as a reason for those changes. Healthcare providers should follow their organization's policies and procedures regarding the disclosure of PHI to patients for reasons other than treatment, payment, and healthcare services.

Patients have the right to know who has accessed their PHI up to 6 years prior to the date the request is submitted.

SPECIAL CIRCUMSTANCES

The Privacy Rule permits the disclosure of PHI without authorization for specified public health services. In situations where public safety is being threatened, it may be necessary to access PHI for reporting purposes.

BUSINESS ASSOCIATES

In 2013, HIPAA expanded its use to include those of business associates. A business associate is an individual or group that manages identifiable health information on behalf of a covered entity, such as in coding, billing, or electronic health records.

BREACH IN PHI

A breach in PHI is an unauthorized access or disclosure of PHI, compromising the privacy of the affected individual. The HIPAA Breach Notification Rule requires prompt notification to affected individuals and the Secretary of Health and Human Services that a breach has occurred. Healthcare providers should alert their supervisor immediately upon any known security breach. Organizations should have a contingency plan in place in the event of a potential or an actual security breach.

PENALTIES FOR HIPAA VIOLATIONS

The U. S. Department of Health and Human Services' Office for Civil Rights and State Attorney General are responsible for enforcing HIPAA Privacy and Security Rules and conducting violation investigations.

Civil Monetary Penalties under the HIPAA Final Rule		
Violation Category	**Per Violation(Minimum)**	**Maximum Civil Money Penalties for Violations**
Did Not Know - (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Reasonable Cause (not due to willful neglect)	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected (within required time period)	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect (not corrected)	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Criminal Penalties for HIPAA violations	
Violations for Non-Compliance Criminal Penalties	• Up to $50,000 and 1 year in prison for improperly obtained or disclosed PHI • Up to $100,000 and up to 5 years in prison for offenses committed in obtaining PHI under false pretenses • Up to $250,000 and up to 10 years in prison for offenses committed in disclosing PHI with the intent to sell, transfer, or use this information for commercial advantage, personal gain, or malicious harm

SAFEGUARDING RECOMMENDATIONS

A covered entity should:

- Ensure conversations (hand-off communications) regarding patients are done in a confidential area.
- Avoid discussing a patient's condition in front of other patients, visitors, or family members in a hallway.
- Lower voice when discussing patient information in person and/or over the phone.
- Avoid having conversations about patients in public places, such as elevators, public hallways, or the cafeteria.
- Ensure that patient-related information is not visible to the public, i.e., computer screens, etc.
- Sign off of computers when not in use.
- Use passwords on desktops and portable media devices.
- Change passwords, as often as organization's policy allows.
- NEVER share passwords.
- Ensure data encrypted computers are used when handling PHI.
- Keep PHI secure i.e., password protecting computers, locking filing cabinets or rooms, etc.
- Use precautions to protect PHI from accidental disclosure.
- Avoid sending PHI by e-mail if at all possible.
- Use a fax cover sheet when faxing PHI, reconfirming fax numbers are correct before sending.

HITECH ACT

The Health Information Technology for Economic and Clinical Health Act (The HITECH Act) was implemented in 2009 as part of the American Recovery and Reinvestment Act of 2009.

The HITECH Act is an amendment to HIPAA with a focus on increased security and privacy of electronically transmitted health information (electronic health records).

An EHR (electronic health record) is an electronic format of a patient's medical record that is maintained by the provider. The EHR improves efficiency of clinical processes and automatic information transfer.

HOW HITECH APPLIES TO CAREGIVERS

- Increases development and use of EHR in the workplace
- Increases development and monitoring of EHR security in the workplace; in other words, ensures who accesses EHR has a need to know
- Requires immediate reporting of any and all EHR security breaches
- Increases penalties for discovered breaching safeguards contained in the Security Rule
- Requires HHS to conduct periodic audits
- Imposes mandatory penalties for willful neglect

HIPAA was established to secure and maintain the security and privacy of patient information. It is the responsibility of every individual to know an organization's policies and procedures where they work and to practice appropriate security measures outlined in this training document to ensure the privacy of all personal health information.