Access 2 Care

A Global Medical Response Solution

HIPAA and Safeguarding PHI

Access2Care
A Global Medical Response Solution

INTRODUCTION

- In the U.S., the health information of individuals is federally protected. This protection is enforced by the U.S. Department of Health and Human Services and mandated by the Health Insurance Portability and Accountability Act or HIPAA.
- Violating a privacy regulation of HIPAA can result in civil and/or criminal penalties. Criminal penalties can range from $50,000 to $250,000 and imprisonment from 1 to 10 years.
- This module discusses HIPAA and its related acts such as Health Information Technology of Economic and Clinical Health (HITECH).

HIPAA

- With the overwhelming popularity of social media platforms and ever-growing threat of cyber-attacks, it has become imperative for healthcare organizations to understand how to appropriately safeguard PHI.
- The Department of Health and Human Services' Office for Civil Rights (OCR) has the authority to levy financial penalties to healthcare organizations as well as healthcare practitioners for HIPAA violations. OCR considers a number of factors before issuing penalties for HIPAA violations. These factors include:
  - The length of time a violation persisted
  - The number of people affected
  - The nature of the data exposed
- Civil penalties can be imposed for violations of HIPAA rules. The penalty amount can range from $119 to $59,522 per violation, with a calendar year cap of $1,785,651

Access2Care
A Global Medical Response Solution

WHO IS COVERED UNDER HIPAA

- Any health plan, healthcare clearinghouse, or any healthcare provider (including transportation providers) who transmits certain health information in electronic form in connection with treatment, payment, or healthcare operations is a covered entity. For example, clinicians, hospitals, ambulance companies, transportation companies and drivers, and billing companies.
- HIPAA covers Individually Identifiable Health Information (IIHI) and refers to this information as Protected Health Information (PHI). Generally, the person who is the subject of the PHI has the right to privacy. However, at times, it is the ‘personal representative’ who can exercise the privacy rights of the patient.
- Personal representatives can include parents, guardians, and others. The personal representative is a person with legal authority to make healthcare decisions on behalf of the individual.

WHAT IS COVERED UNDER HIPAA

- PHI includes demographic or other identifying information which is created or received by another covered entity, and:
  - Relates to the past, present, or future physical or mental health condition of an individual; or
  - Relates to the provision of healthcare to the individual; or
  - The past, present, or future payment for the provision of healthcare to the individual and identifies the individual; or
  - Provides a reasonable basis to believe the information can be used to identify the individual.

ELEMENTS IN PHI

The various elements covered in PHI are:

- Name
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
  - The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
  - The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
- All elements of dates (except year) that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers, fax numbers and e-mail addresses
- Social security numbers
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full-face photographs and any comparable images
- Any other unique identifying number, characteristic, or code

Access2Care
A Global Medical Response Solution

HIPAA GUIDELINES

- HIPAA regulations limit when and how we use and disclose PHI. We ‘use’ PHI when we internally share, examine, or analyze an individual’s health information. We ‘disclose’ PHI when we release, transfer, or give access to PHI to another entity.
- Individual authorization for disclosure of information requires a written permission from the patient. However, for treatment, payment, or healthcare operations (TPO), we may use and disclose PHI without the individual’s permission.
- The two basic ways of disclosing PHI is through oral communication and electronic communication.

ORAL COMMUNICATION

- The HIPAA Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, healthcare providers may engage in communications as required for quick, effective, and high-quality healthcare, even if there is a possibility that they could be overheard. Any disclosure that is overheard during information transfer is called “incidental disclosures”.
- Incidental uses and disclosures of PHI are not considered violations of the HIPAA Privacy Rule provided that reasonable precautions to safeguard the information have been taken. Some of these precautions are:
  - Speaking quietly when discussing a patient’s condition with family members in a waiting room or exam area;
  - Avoiding use of a patient’s name in public hallways and elevators; and
  - Avoiding discussion of the patient’s condition with bystanders.

ORAL COMMUNICATION

- **Protection:**

Co-workers and former co-workers of covered entities have the same privacy rights any other individual has under the HIPAA regulations. In the event an employee, co-worker, or former employee seeks treatment at a medical or psychological facility, employees must use the same measures to protect their confidentiality as they would in the case of any other patient. They must also refrain from mentioning the presence or condition of this person to any other co-worker or employee.

- **Videotape/Photographs:**

Clinicians should refrain from videotaping or photographing any aspect of the interaction with a patient that could result in the use or disclosure of the patient's PHI in any form (oral, written, or electronic) without prior written approval from the Chief Compliance Officer and the Law Department. Do not use your camera phone or recording devices for anything involving a patient or patient care unless the recording is in accordance with Company policy.

- **Transmission:**

Do not use text messaging or e-mail to disclose PHI to others unless in accordance with Company policy and encryption standards. Text messaging or e-mailing through unsecure means (i.e., personal e-mail accounts, etc.), may result in a HIPAA violation.

ELECTRONIC COMMUNICATION

- Today, a lot of individuals use social media and electronic communication to better communicate with patients, co-workers and/or for their own personal use.
- While social media offers great opportunities for personal and timely communication, the danger lies in the ease with which people accept and utilize this new medium. Healthcare providers and employees must apply caution to protect the privacy and trust that patients expect, and the law requires. Some of the safeguard measures are:
  - Periodically check your privacy settings, preferably once a week, as they can change.
  - Use passwords to access information stored electronically.
  - Safeguard personal data and other portable electronic devices.
  - Never refer to a patient by name, and do not give out information that could identify the patient.
  - When referencing a particular case, conditions, or treatments, be as general as possible. Do not describe specific demographics or populations that can be identified.
  - Be careful of language used in e-mails or documentation.

SOCIAL MEDIA

- Viewing social media has become a norm for individuals in today's world, and healthcare professionals are no different. Research shows that over 30% of healthcare professionals not only view social media content but also use these platforms to socialize with others either in or outside of the healthcare field. However, with such widespread use of these platforms, it is important to remember that PHI should not be disclosed on any social media platforms.
- As per the HIPAA Privacy Rule, a violation or breach occurs when PHI is used or disclosed without appropriate authorization.
- Here are some examples of common social media mistakes that could lead to violations under the HIPAA Privacy Rule.
  - Uploading patient images and videos without their written authorization
  - Posting details or gossip about a patient or patient condition
  - Posting any information that could lead to a patient being identified
  - Uploading images where the patient or his/her PHI is visible
  - Sharing texts, images, or videos about a patient's PHI

PHISHING

- Phishing is a threat to the confidentiality, integrity, and availability of ePHI and PII. All covered entities are expected to take appropriate security measures to safeguard PHI under HIPAA.
- Phishing is a type of cyberattack that is deployed through a disguised email with the purpose of tricking the email recipient into sharing or disclosing sensitive information.
  - A cyber-criminal could use a phishing attack to gain access to a healthcare company's records, including patient or employee information, such as social security number, medical information, and insurance information.
- The number of attempted phishing attacks in the healthcare industry continues to increase as protected health information is valuable in the black market. What happens following a successful phishing attack?
  - GMR IT Security is notified and a review is conducted.
  - GMR IT Security may engage a forensic reviewer to determine exposure of Protected Health Information (PHI) and/or Personally Identifying Information (PII).
    - Tip: Save emails that include PHI or PII to a secure company shared drive and delete the email from your inbox.
  - The Compliance Dept. will determine if state and government reporting is warranted
  - The Compliance Dept. will determine if breach notifications to patient, employees, media and/or the U.S. Dept. of Health and Human Services are warranted

VERBAL DISCLOSURES

- The HIPAA Privacy Rule provides consumers with important privacy rights and protections with respect to their health information, including important controls over how their health information is used and disclosed by health plans and healthcare providers.
- Healthcare providers may engage in communications as required for quick, effective, and high-quality healthcare, even if there is a possibility that they could be overheard. Any disclosure that is overheard during information transfer is called “incidental disclosures.”
- Incidental uses and disclosures of PHI are not considered violations of the HIPAA Privacy Rule provided that reasonable precautions to safeguard the information have been taken. Some of these precautions are:
  - Speaking quietly when discussing a patient’s condition with family members on scene or in an exam area.
  - Avoiding use of a patient’s name in public or with parties who don’t have a need to know.
  - Avoiding discussion of the patient’s condition with bystanders.

HIPAA SECURITY GUIDELINES

- HIPAA security guidelines that all healthcare providers should comply with are as follows:
  - Establish formal policies and procedures to protect electronic Protected Health Information (ePHI).
  - Ensure passwords and usernames are not easily accessible to individuals who do not have access to electronic records.
  - Safeguard any personal devices that may house protected information.
  - Ensure paper medical records are maintained within a locked and secured area.
  - Position computer monitors to prevent easy viewing by individuals who are not authorized to see patient data.
  - Lock your computer when you get up from your workspace.
  - Encrypt company emails containing protected health information by simply including *secure* in the subject line.

Access2Care
A Global Medical Response Solution

PATIENT RIGHTS UNDER HIPAA

- HIPAA gives individuals the legal right to have more control of how their PHI is used or disclosed. The regulation also establishes deadlines in responding to requests for access, amendments, and accountings of the patient's PHI and requires healthcare companies to implement procedures for reviewing denials of those requests.

PATIENT RIGHTS GUIDELINES

- **Right to Inspect and Copy:**

HIPAA gives individuals the legal right to see and obtain a copy of their own PHI for as long as the covered entity maintains the information. In general, the covered entity must allow an individual to inspect or obtain a copy of the PHI no later than 30 days after receiving the request.

Individuals must make all requests for access to PHI in writing. In addition, the covered entity must keep all written requests for access to PHI with the medical record for as long as they maintain the record.

- **Right to Amend:**

HIPAA gives individuals the right to amend or supplement their own PHI. For example, an individual who disagrees with a medical opinion can submit a second opinion to be included in the medical record. The individual has this right for as long as the covered entity maintains the information. Individuals must submit all requests for amendments in writing.

The covered entity may deny an individual's request for amendment, for example, if the entity determines that it did not create the information or that the information would not be available for inspection because the individual does not have a right to access.

PATIENT RIGHTS GUIDELINES CONT.

- **Right to Request Restrictions:**

Under HIPAA, an individual has the right to request restrictions on the uses or disclosures of the PHI. For example, an individual may request that a particular medical procedure be kept confidential and not shared with other providers. Although the covered entity is not required to agree to such a restriction, if they enter into an agreement to restrict, they must abide by the agreement, except in emergency circumstances.

- **Right to Request Itemized Details:**

Individuals have the right to receive an itemized list of disclosures of their PHI made by the covered entity during six years prior to the date that the individual requests the accounting, including disclosures to or by business associates. This should include the following:

  - The date of each disclosure
  - The name and, if known, the address of the organization or person who received the information
  - A description of the information disclosed
  - A statement of the purpose of the disclosure

Access2Care
A Global Medical Response Solution

HITECH ACT OF 2009

- The U.S. Department of Health and Human Services (HHS) implemented the HITECH Act in 2009. The Department's implementation of these HITECH Act enforcement provisions strengthened the HIPAA protections and rights related to an individual's health information.

OVERVIEW OF HITECH ACT

- The HITECH Act significantly increased the penalties the Secretary of HHS may impose for violations of the HIPAA rules. It establishes a tiered range of increasing civil penalty amounts, with a maximum penalty of $1.5 million for all violations of an identical provision.
- HITECH requires that covered entities provide notification to individuals when there is a breach of unsecured (paper or electronic) PHI. Notifications must be distributed to:
  - The patient
  - The Department of Health and Human Services
  - The Media in limited situations
  - Other entities as required by state laws

FAQS ON BREACH

- **What is a Breach?**

An impermissible acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI.

- **What would be good examples of potential breaches?**
  - Theft of an unencrypted laptop
  - Theft of patient's medical records
  - A patient's receipt of another patient's medical records containing the original patient's name, social security number, address, and medical information
  - ePHI obtained through a company's computer system by an unauthorized individual
- **What are exceptions to the breach rule?**
  - Unintentional good faith acquisition, access, or use of PHI by a workforce member
  - Inadvertent disclosure between two individuals who are otherwise authorized to access the PHI
  - Disclosure to an unauthorized person for such a short time that the unauthorized person would not reasonably have been able to retain the information

FAQS ON BREACH CONT.

- **What should a healthcare worker do if they believe a co-worker has committed a HIPAA violation?**

Report it to the Company's Privacy Officer or Compliance Department.

- **When is a Breach Notification Warranted?**

Covered entities must presume that notification is required in all circumstances, except when the covered entity conducts a risk assessment that establishes that there is a 'low probability' of comprise of the PHI.

Access2Care
A Global Medical Response Solution

HIPAA Assessment

Thank you for reviewing the training. Now click on the link below to take the test.

https://amr-svwzg.formstack.com/forms/hipaa_training_tp_portal