Simplifying Healthcare Administration

HIPAA PRIVACY TRAINING

Health Insurance Portability and Accountability Act

July 2023

OBJECTIVES

- Protecting Privacy and Security
- Review key terms and definitions
- Understand when it is appropriate to access Member/Patient information – “Minimal Necessity Rule”
- Member Rights
- Understand your role for identifying and reporting HIPAA Privacy and Security issues

PROTECTING

- Members/Patients routinely share personal information with health care providers. If the confidentiality of this information is not protected, trust in the physician-patient and healthcare relationship would be affected.

PRIVACY & SECURITY

Health care entities must take steps to ensure that Member/Patient protected health information (PHI) is not viewed by anyone without “a business need to know,” and is not stolen, lost, or accidentally destroyed.

Posting ANY member information or photos even without names may lead to termination, fines and jail time

KEY TERMS

What is HIPAA?

Health Insurance Portability and Accountability Act of 1996 is a federal law that required the creation of national standards to protect patient health information (PHI) from being disclosed without the patient's consent or knowledge.

KEY TERMS

What is PHI?

Protected Health Information (PHI) is information that relates to a member's/patient's past, present or future physical or mental health care or condition, including any payment for physical or mental health care, as well as any associated personally identifying information (PII)**

** **PII** - A general term used to describe any form of sensitive data that could be used to identify or contact an individual. For example, any payment or authentication information (i.e., mother's maiden name) is considered PII. When PII is used in connection with a member/patient's physical or mental health care or condition or payment for said care, PII becomes PHI.

KEY TERMS

What types of PHI are protected?

- Paper Records
- Electronic Records
- Oral Communication
- Fax/Email documents
- *Any* information that can identify the member and is related to the person's past, present or future physical or mental health condition
- Anything associated with healthcare services or treatment

IDENTIFIERS

THE DEPARTMENT OF HEALTH CARE SERVICES (DHCS) LISTS THE 18 HIPAA IDENTIFIERS THAT ARE CONSIDERED PERSONALLY IDENTIFIABLE:

- Names
- Address / Geographic area
- All elements of dates such as Date of Birth, Admit / discharge date, Date of Death
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical Records numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- VIN and serial numbers, including license plate numbers
- Device identifiers and serial numbers

https://www.dhcs.ca.gov/dataandstats/data/Pages/ListofHIPAAIdentifiers.aspx

IDENTIFIERS (CONT.)

THE DEPARTMENT OF HEALTH CARE SERVICES (DHCS) LISTS THE 18 HIPAA IDENTIFIERS THAT ARE CONSIDERED PERSONALLY IDENTIFIABLE:

- Web URLS
- IP address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code, except as permitted

https://www.dhcs.ca.gov/dataandstats/data/Pages/ListofHIPAAIdentifiers.aspx

MEMBER RIGHTS

Mandated by HIPAA, members have the right to:

- Receive the Notice of Privacy Practice
- Access their medical records
- Request amendments to their medical records
- An accounting of disclosures of their medical records
- Request restrictions on release of PHI
- File a complaint

MEMBER RIGHTS (CONT.)

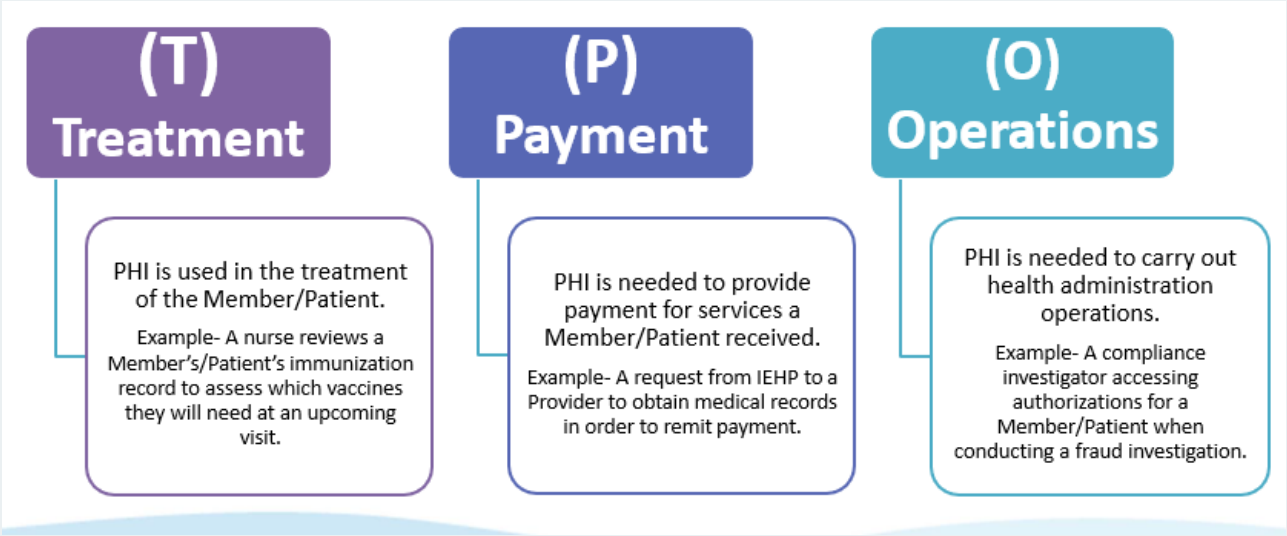
<<Health Plan and/or Delegate to fill in the name/number of the policies below and include access link if available>>

<<LIST YOUR COMPANY MEMBER RIGHTS POLICY NAME/NUMBER HERE>>

ACCESSING PHI

The law allows access and disclosure of Member/Patient PHI when a request or need for information falls under Treatment, Payment or Operations (TPO).

Access to PHI without member/patient authorization is not limited to TPO (see 45 CFR 164.502).



MINIMUM NECESSARY RULE

Understand when it is appropriate to access Member/Patient information

"Minimum Necessary" Rule

- Clinical staff, physicians and employees are required to access only the information *they need to do their job* for treatment, payment or healthcare operations (TPO)
- Release of PHI without a signed Authorization Form is not permitted
- Access to your family/friends' records is not permitted without a signed Authorization Form from the member

45 CFR 165.500 seq

YOUR ROLE IN PROTECTING

HICE
health industry collaboration effort

1. Only access information your job REQUIRES for TPO (Treatment, Payment, Healthcare Operations)
2. Prior to release of PHI, ensure Authorization Form is obtained (as needed for compliance with the Privacy Rule)
3. If transmitting PHI electronically, ensure that you are sending the transaction through a secure portal or through a secure email
4. If faxing is required, a cover sheet can be sent to a physician office or other health care facility's fax machine that is within a secure location. Before faxing, make sure to:
    - Confirm the fax number prior to sending
    - Send fax to approved fax numbers, or make sure the recipient is waiting by the machine to receive the fax
    - If sent to an inappropriate fax number, report the matter to your supervisor immediately

YOUR ROLE IN PROTECTING (CONT.)

5. Do not share member information in open areas where you can be overheard by others
6. Lock your computer *every* time you walk away, and/or log off at the end of the day
7. Do not share or disclose member information with family, friends or co-workers
8. Do not email, post or text (including photos) anything that can identify a member
9. Know the permission level granted by the member in order to leave a HIPAA-compliant voice message
10. Know how and where to dispose of all PHI – shred, locked bins, etc.
11. PROMPTLY REPORT MEMBER PRIVACY INCIDENTS to your supervisor, privacy officer per your company policy

<<Health Plan and/or Delegate to fill in the name/number of the policy below and include access link if available>>
<<LIST YOUR COMPANY POLICY NAME/NUMBER HERE>>

SECURE EMAILS

- Securing Emails is mandatory for all HIPAA protected information going outside <company name>

LEAVE BLANK FOR HEALTHPLAN

OR DELEGATE TO FILL IN their process for secure emails

OVERSIGHT

Oversight of HIPAA and security is:

LEAVE BLANK FOR <company>

OR DELEGATE TO FILL IN. INCLUDE HOW TO REPORT ANONYMOUSLY

DISCLAIMER

This course was prepared as a service and is not intended to grant rights or impose obligations. This course may contain references or links to statutes, regulations or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. Readers are encouraged to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

POST-ASSESSMENT QUIZ

1. The primary Federal Law pertaining to the medical information privacy is:
   a. American Recovery and Reinvestment Act (ARRA)
   b. Health Information Technology for Economic and Clinical Health Act (HITECH)
   c. Health Insurance Portability and Accountability Act (HIPAA)
   d. All of the above
   e. None of the above
2. What is PHI?
   a. Privacy Health Information
   b. Protected Health Information
   c. Patient Health Insurance
3. Which of the following are examples of PHI?
   a. Patient's Name
   b. Patient's Date of Birth
   c. Patient's Address
   d. Medical Record Number
   e. Admission date, time, and reason
   f. All of the above
   g. None of the above

POST-ASSESSMENT QUIZ

4. The “minimum necessary” requirement of HIPAA refers to using or disclosing/releasing only the minimum PHI necessary to accomplish the purpose for which it is being used, requested, or disclosed.
    a. True
    b. False
5. The HIPAA Privacy Rule protects all PHI, electronic, verbal and written.
    a. True
    b. False
6. If you need to report a HIPAA concern or violation, which of the following can you do?
    a. Contact my organization’s HIPAA Compliance Officer
    b. Contact my supervisor or manager
    c. All of the above
    d. None of the above

POST-ASSESSMENT QUIZ

7. HIPAA mandates that members have the right to:
    a. Request restrictions on release of PHI
    b. File complaints
    c. Receive the notice of privacy practices
    d. Access medical records
    e. All of the above
    f. None of the above

8. It is not mandatory to secure emails for HIPAA protected information on outgoing email
    a. True
    b. False

9. Only access the information your job requires for treatment, payment, Healthcare Operations
    a. True
    b. False

10. An authorization form is not needed prior to releasing PHI
    a. True
    b. False