Health System One | Health Network One | Therapy Network | Eye Management

2021 Health Insurance Portability and Accountability Act (HIPAA) Training

HIPAA

HIPAA was enacted to improve the efficiency and effectiveness of the health care systems through the **establishment of standards and requirements for the electronic transmission** of protected health information (PHI).

- HIPAA is overseen by the Department of Health & Human Services (HHS) and enforced by the Office of Civil Rights (OCR).

The Health Information Technology for Economic and Clinical Health Act (HITECH) was signed to promote the adoption and meaningful use of health information technology.

Omnibus: Final Rule

The Final Rule harmonizes the requirements of HITECH in the HIPAA Law.

- Establishes fundamental changes to the definitions of business associates and breach of PHI.
- Expands the individual's rights to access PHI.
- Includes new provisions for the Notice of Privacy Practices.
- Allows the sale of PHI.
- Introduces the figure of subcontractors.
- Applies part of the Privacy Rule to business associates.
- Prohibits the use of genetic information for underwriting purposes.
- Establishes new terms for the protection of PHI for deceased individuals.
- Allows the disclosure of student immunization records, if required by the schools, without requiring writing authorization.
- Imposes new civil money penalties to covered entities and business associates for noncompliance with HIPAA.
- Applies the Security Rule to business associates.

Privacy Rule

Purpose:

- Protects the confidentiality of PHI in all formats (paper, verbal, and electronic).
- Grants the members understanding and control of how their PHI is used.
- Ensures that PHI is used for health purposes only.
- Establishes that PHI can only be disclosed for treatment, payment, or health care operations (TPO) or with the consent (valid authorization) of the individual.
- Establishes individual's rights with respect to their health information.
- Establishes the notification process for HIPAA Breaches.

Who is covered by HIPAA?

- Health Plans
- Healthcare Providers and Institutions: physicians, hospitals
- Health care Clearinghouses: central institutions that establish transactions.
- HIPAA requires that covered entities use or disclose PHI in a limited way. Under the HIPAA minimum necessary standard, HIPAA-covered entities are required to make reasonable efforts to ensure that access to PHI is limited to the minimum necessary information to accomplish the intended purpose of a particular use, disclosure, or request.

Minimum Necessary

45 CFR 164.502 (b), 164.514 (d)

The minimum standard requirement **does not apply to**:

- Disclosures to, or requests, by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- De-identified information.
- Uses or disclosures required by law.
- Among others.

What is protected by HIPAA?
Protected Health Information (PHI)

PHI is individually **identifiable health information** collected from an individual, created or received by a covered entity and:

- Related to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or to the past, present, or future payment for the provision of health care to an individual; and
- **Identifies the individual** or could identify the individual.
- Could be transmitted or maintained electronically, or through any other medium.

Identifiers of PHI

Information that can be used to identify, contact, or locate an individual.

- Names
- Geographic data
- Information that can be used to identify, contact, or locate an individual.
- All elements of dates
- Telephone number
- Fax Numbers
- Email address
- Social Security Number
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Device identifiers and serial numbers
- Web URLs (Uniform Resource Locater)
- Internet protocol addresses
- Biometric identifiers (e.g. retinal scan, fingerprints)
- Full face photos and comparable images
- Any unique identifying number, characteristic or code

What does the Privacy Rule require providers and health plans to do?

- Notify the individuals about their privacy rights and how their information can be used and disclosed.
- Adopt and implement processes in their practices, hospitals, or plan.
- Train their employees to understand the privacy processes.
- Designate a responsible person to ensure that the privacy processes are applied and followed.
- Ensure that the records containing PHI are not exposed or available for use by unauthorized persons.

Permitted Uses and Disclosures of PHI

45 CFR 164.502

The use and disclosure of PHI is permissible:

- For **TPO**: treatment, payments and healthcare operations.
- When a **valid written authorization** exists from the individual, authorizing the use and disclosure of his/her PHI to a third party (representative).
- To a family member or friend that is involved with the medical care or payment of the medical care of the individual and the individual has the opportunity to accept/object the use or disclosure.
  - For health oversight activities.
  - When it is required by law.
  - For law Enforcement Purposes or National Security.
  - For judicial and administrative proceedings.
  - For Forensic Pathologist, Judges and Funeral Directors.
  - To avert a serious threat to health or safety.
  - Among others.

Notice of Privacy Practices (NPP)

45 CFR 164.520

A document that explains the individual's rights to their PHI, the legal duties and privacy practices of the covered entity with respect to the individual's PHI, and the ways in which the covered entity may use or disclose such information.

- A health plan must distribute its privacy practices notice to each new enrollee at the moment of enrollment and send a reminder to every enrollee at least once every three years.
- A health plan must make its notice electronically available in their website.

Sale of PHI

45 CFR 502 (a) (5) (ii)

Do not accept remuneration for PHI **without the individual's authorization** unless it is to recover the costs of providing data to a Public Health Officer, an Investigator or the individual himself, or to comply with certain other exceptions.

Restriction of Marketing

45 CFR 164.501 and 164.508 (a) (3)

Follows these guidelines when sending marketing materials:

- Do not send an individual marketing materials and get paid for it, unless he/she authorized it or he/she is taking the medicine being marketed.
- Do not send an individual marketing materials for free, unless he/she authorizes it or the communication is made for certain purposes (i.e. to describe a product available in the health plan or to recommend an alternative health care option).

PHI of a Deceased Individual

- The period of protection of PHI of a deceased individual is up to 50 years. This is a protection term, not a record retention period.
- HIPAA allows the disclosure of PHI of a deceased individual to a family member or close friend who was involved in the individual's care or payment of healthcare prior to the individual's death, unless doing so is inconsistent with any prior expressed preferences of the individual.

Psychotherapy Notes

45 CFR 164.508 (a) (2)

A covered entity must obtain individual's authorization to use or disclose psychotherapy notes except:

- The covered entity who originated the notes may use them for treatment, for its own training, or to defend itself in legal proceedings brought by the individual.
- For HHS to investigate or determine the covered entity's compliance with the Privacy Rule.
- To avert a serious and imminent threat to public health or safety.
- To a health oversight agency for lawful oversight of the originator of the psychotherapy notes.
- For the lawful activities of a coroner or medical examiner or as required by law.

Individual's Rights under HIPAA

Right of Access:

The Privacy Rule required Covered Entities (e.g. health plans) to provide individuals, upon request, the right to **inspect or obtain a copy** of their PHI in one or more "designated record sets" maintained by or for the covered entity. (45 CFR 164.524)

- A covered entity must act on a request for access no later than 30 days after receipt of the request. An extension of 30 days can be made notifying the individual making the request.
- The plan can send a copy of the PHI directly to a third person designated by the individual, if such request is made in writing, providing the name and address of the third party.

Right to Amend or Correct PHI:

Individuals have the right to have covered entities **amend** their PHI in a designated record set when that information is inaccurate or incomplete. (45 CFR 164.526)

- Covered entities must respond to a request for an amendment within 60 days.

Individual's Rights under HIPAA

Right to Disclosures of Accounting of PHI:

Individuals have a right **to an accounting of the disclosures** of their PHI by a covered entity or the covered entity's business associates except the disclosures made for one the following reasons:

- Treatment, payment, or healthcare operations (TPO), pursuant to a valid authorization, to the subject of the information, for national security purposes, to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody, incident to otherwise permitted or required uses or disclosures. (45 CFR 164.528)
- Request of an accounting of disclosures of PHI must be acted on no later than 60 days after receipt of the request. An extension of 30 days can be made notifying the individual making the request.

Individual's Rights under HIPAA

Request of Restrictions:

Individuals have the right to request that a covered entity **restrict** uses or disclosures of PHI for treatment, payment or health care operations (TPO), disclosures to persons involved in the individual's health care or payment for health care, or disclosures to notify family members or others about the individual's general condition, location, or death. (45 CFR 164.522 (a)).

- The plan is under no obligation to agree to requests for restrictions. However, if the plan does agree, it must comply with the agreed upon restrictions, **except** for purposes of treating the individual in a medical emergency and the restricted PHI is needed to provide the emergency treatment.

Individual's Rights under HIPAA

Confidential Communications:

The plan must permit members to request **an alternative means or location** for receiving communications of PHI by means other than those that the plan typically employs. (45 CFR 164.522 (B))

- For example: A member can request that the health plan communicate with the individual through a designated address or phone number.

Health Plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the PHI could endanger the individual.

Breach of PHI

45 CFR 164.402

A breach is any **unauthorized acquisition, access, use or disclosure** of PHI which compromises the privacy and security of the PHI.

- The information was accessed, acquired, used or disclosed in a manner not permitted by the Privacy Rule.

The use or disclosure of PHI not authorized by HIPAA is **presumed** to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been **compromised**.

HIPAA Breach Exceptions

Does not constitute a HIPAA breach:

- Unintentional acquisition, access, or use of PHI by an employee or other person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of authority and does not result in further use or disclosure in a manner not permitted by HIPAA.
- Inadvertent disclosure of PHI:

  a) From one person authorized to access PHI at a covered entity or business associate

  b) To another person in the same facility

  c) As long as the PHI is not further disclosed.
- Disclosure of PHI to an unauthorized person in which it is not reasonable for that person to have retained such information.

Risk Assessment to determine likelihood of PHI compromise

- Probability of PHI compromise may only be determined through a breach risk assessment considering the following factors:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
  - The unauthorized person who used the PHI or to whom the disclosure was made.
  - Whether the PHI was actually acquired or viewed.
  - The extent to which the risk to the PHI has been mitigated.
- Covered entity/business associate has the burden of proof to demonstrate that all notifications were made or that notifications were not required.

PHI Breach Examples

- Unauthorized disclosure of PHI to a third party in paper or electronically (without a valid authorization).
- Lost, stolen, or improper disposition of documents with PHI.
- Access of PHI for an improper purpose by an unauthorized person.
- The sending of unprotected PHI outside of the company (e.g. without encryption) giving an unauthorized person access to the information.
- Theft/loss of any of the organization's equipment including computers, monitors, mobile phones, and USBs.
- Unauthorized access or use of information.

Security Rule

45 CFR PART 160 and Subparts A and C of Part 164

Purpose:

- The security rule requires covered entities to protect PHI in electronic form (ePHI).
- Establishes controls to safeguard the confidentiality, integrity, and availability (CIA) of ePHI.
  - **Confidentiality:** ensuring that ePHI is not made available or disclosed to unauthorized persons.
  - **Integrity:** ensuring that the ePHI input today is the ePHI that is retrieved in the future (ePHI has not been altered or destroyed in an unauthorized manner).
  - **Availability:** ensuring that ePHI is available to those who need it, when it's needed.
- Intended to protect ePHI against any reasonably anticipated threat or hazard, and improper use or disclosure.

Password Management

- Create a unique, strong password or PIN for each account or device and keep your credentials secure.
  - Don’t use personal or easy-to-guess information when creating a password.
  - Make a password complex by adding numbers, multi-case letters (upper and lower), and symbols.
  - Mix numbers into the center of your password.
- Password Policy Guidelines - A minimum of 8 characters long and contain at least a mix of THREE of the following FOUR properties:
  - Lowercase letters (a-z)
  - Uppercase letters (A-Z)
  - Numbers (0-9)
  - Symbols (!”Â£$%^&*)
- Strong password examples:
  - B5rCo5#44E4
  - M1c3nm3n
  - Goo*stov

Password Management (continued)

Don't:

- Reveal your password to anyone.
- Share your password to your supervisor, Service Desk employee, or a family member.
- Allow anyone else to use your User ID and password.
- Reveal your password on questionnaires or security forms.
- Store your passwords in a file on any computer system.
- Re-use the same password
- Write your passwords down and store them anywhere in your office.
- Place your passwords into email messages or other forms of electronic communication.

Remember: Change all passwords frequently and keep your passwords secret.

Civil Money Penalties

OCR new interpretation of HITECH, penalties are applied based on level of culpability and breaches will be penalized under one of four tiers:

1. Parties completely absolved of all culpability in the breach will be fined a maximum of $25,000 per year.
2. Those who did not willfully violate HIPAA but experienced a breach due to “reasonable cause” will be limited to $100,000 in annual fines.
3. Breaches that occurred due to “willful neglect” but were rectified in a timely manner will be fined up to $250,000.
4. The $1.5 million yearly cap will still apply to the highest-tier violations, which are caused by willful neglect and are not corrected as soon as possible.

Office for Civil Rights (OCR)

Anyone can file a written complaint with the OCR by mail, fax, or email:

The OCR toll free number is 1-800-368-1019

Address: Region II - NJ, NY, PR & VI
Office of Civil Rights
US Department of Health & Human Services
26 Federal Plaza- Suite 3313
New York, NY 10278

212-264-3313, 212-264-2355 (TDD), 212-264-3039 (Fax)

Webpage: http://www.hhs.gov/ocr/privacy

Remember: Use of Email

- Emails containing PHI must be sent secured and encrypted.
- As an information security measure, do not use your personal emails to receive or share the confidential and protected health information of our members.
- Please follow the guidelines below when sending PHI via email:
  - Include the minimum necessary of PHI to complete the purpose of the message.
  - Ensure that the address of the recipient is correct and that the document included in the message (if any) is correct.
  - Encrypt all emails to external persons outside the company.
  - Do not send PHI in email unless email is encrypted.
  - Never put any PHI in the subject line of emails.

Remember: Management of PHI

- Follow the procedure for the proper disposal of sensitive information using locked recycling drop boxes.
- Keep laptops, smartphones, USBs and any other memory or document containing PHI in a secure place.
- Never leave PHI on your desk in plain sight.
- Make sure not to leave documents that contain PHI in printers or fax machines.
- Use strong passwords. Keep your user ID and passwords confidential and secure. Never share your password or user name (User ID).
- Do not access PHI that you do not need to access.

Report ethical, compliance,fraud, waste, and abuse violations in a confidential manner at:

SIU@healthsystemone.com

1-866-321-5550