Brattleboro Retreat

Introduction to Protected Health Information (PHI) and the Health Insurance Portability and Accountability Act (HIPAA)

Objectives

At the end of this course, you should be able to:

- Identify PHI and how to safeguard it correctly
- Know consumers rights under HIPAA
- How to report a potential HIPAA violation
- Understand the impact of potential violations
- Apply that knowledge using actual HIPAA scenarios

What is Privacy?

The quality or state of being apart from company or observation or freedom from unauthorized intrusion.

Meaning: The right of an individual to have personal, identifiable health information kept private and to control access by other people to that information.

“Privacy.” *Merriam-Webster.com Dictionary*, Merriam-Webster, https://www.merriam-webster.com/dictionary/privacy. Accessed 26 Jan. 2021.

What is PHI?

Protected Health Information (PHI) is any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed to a covered entity and/or their business associate in the course of providing a health care service.

This information can relate to a person’s past, present or future health conditions, including mental health.

Examples are found in the next slide.

PHI Identifiers

The 18 identifiers that make health information PHI are:

- Names
- Dates, except year
- Telephone numbers
- Geographical data
- Fax numbers
- Social Security Numbers
- Email addresses
- Medical Record Numbers
- Account Numbers
- Health Plan Beneficiary Numbers
- Certificate / License Numbers
- Vehicle Identifiers, Serial Numbers, incl. License Plate
- WEB URLs
- Device Identifiers & Serial Numbers
- Internet protocol addresses
- Full face photos & comparable images
- Biometric identifiers, incl retinal scan, fingerprints
- Any unique identifier or code

What agencies protect PHI?

Protected Health Information is protected by Federal laws, including:

- HIPAA
- HITECH – the Health Information Technology for Economic and Clinical Health Act, which is a supplement to HIPPA regulations and part of the American Recovery and Reinvestment Act of 2009.
- Title 42 of the Code of Federal Regulations, Part 2 which relates to confidentiality of alcohol and drug abuse patient records

More about HIPAA

Health Insurance Portability and Accountability Act (HIPAA) was enacted to improve the protection of private information because the current laws were inadequate and inconsistent.

HIPAA prevents disclosure and requires organizations to safeguard their systems as technology advances and medical records moved to electronic media.

HIPAA established nation-wide standards that improved patient record security.

Some of the HIPAA rules are documented on the next slide.

HIPAA has Rules

- The Breach Notification Rule – reporting an “unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information.”
- The Enforcement Rule – standardized procedures and requirements for investigating complaints and imposing monetary penalties
- The Privacy Rule protects PHI
- The Security Rule defines who is covered, what is covered and required safeguards
- The Transactions and Code Sets Rule for electronic data
- The Unique Identifier Rules
- The Information Blocking Rule – to identify entities that place unnecessary obstacles that prevent patients from accessing their medical information

More about HITECH

The Health Information Technology for Economic and Clinical Health Act or HITECH improves privacy, security and liability.

- Imposes civil penalties and conducts audits
- Requires patients and authorities be notified of breaches
- Monitors compliance between business associates concerning safeguards

More Title 42 CFR, Part 2

42 CFR 2, as it is known, outlines penalties for violations of confidentiality for alcohol and drug abuse patient records.

Permission must be given in writing when releasing records that fall under this title. Release of alcohol and drug abuse patient records must be specified in the authorization.

This applies to ALL Retreat records generated prior to January 1st 2024.

How is PHI stored or protected?

- Need to Know – Only the people who need access to a patient's information can access only the parts that affect their job.
- Physical and System Safeguards – such as locked doors, secure computer passwords, closing electronic charts upon completion of documentation, or preventing discussions of patient information publicly.
- Policies and Procedures – Retreat specific policies for all methods of health information must be in place and enforced per HIPAA regulations.

Why should I care?

The easy answer would be because it is required by law, can result in personal fines, and is enforced by Retreat policies.

But, put yourself in the patient's shoes, would you want your nurse or provider to go home and discuss your medical care?

Would you want them to discuss your information with anyone that is not involved in your care?

The right answer should be NO and our patients deserve the same consideration.

PHI Protections

Is accessing this information necessary to do your job?

1. If not, tell your supervisor that you have received the info and that it is not necessary.
2. If you do need PHI, be sure it is for the business at hand and is consistent with BR policies.
3. Try to de-identify information whenever possible to reduce the risk of disclosure
4. When you no longer have business with a patient’s PHI, be sure that all copies of documentation have been appropriately destroyed or deleted.

Safeguards

Safeguards that BR has in place that protects PHI from inappropriate use:

- Education
  - Laws at the state and federal levels
  - BR Policies which can be found in iConnect
  - Procedures – ask your Supervisor for more information
- Restrictions, which includes system passwords
- Paper procedures for handling, storage and destruction of records
- Reporting guidelines
  - Start with your Supervisor
  - Call Medical Records at x 3728

Passwords

- Your passwords are confidential
- Do not share them
- Do not leave them written down where they can be seen or emailed or posted
- You are responsible for **everything** that happens with your Username and Password

Test your knowledge

- You are charting in a patient’s chart; you are called away to deal with a patient situation in another area of the unit. What do you need to do to safeguard this patient’s information?

- You need to make sure you are logged off or that the computer is closed so that no medical information is exposed.

Paper

- All paper documents that contain PHI must be filed and stored according to BR policy and procedure to limit unauthorized access.
- Print using “Secure Print”
- Cover any documents with PHI if an unauthorized person approaches your desk.
- Dispose of documents that are no longer needed as instructed on your unit.

Test your knowledge

- You need to print medical information from a patient’s chart. You pull up the information and hit the print button. Your phone rings, you answer the call and take care of the caller’s request. This request requires you to do some research and is a top priority. You shift your focus to this request and do not go to the printer to retrieve the medical information that you printed.
- What mistake did you make in printing this information that is a Privacy violation under HIPAA?
- Always use “Secure Print” when printing any medical information to protect it from unauthorized disclosure

Talking about PHI

Discussing client information with a coworker who does not need to know within the organization or with anyone outside of the organization is a violation.

Remember: only discuss client PHI with an authorized employee or individual who has a legitimate need to know and has been verified as having the authority to request and receive the information.

Remember:

- If it seems suspicious, talk to your supervisor
- If you suspect a violation, talk to your supervisor or enter an event into Verge
- If PHI is been given out by mistake or incorrectly, enter the event into Verge and inform your supervisor
- Ways to contact your supervisor include telephone, email or in person.

Communications

- Emails, voice messages and any other type of communication should contain only the minimum necessary amount of client PHI for the purpose and only be communicated with those individuals that have a business need to know that information.

- PHI transmitted by email outside the organization should be sent in an encrypted format. This includes any PHI within the body of the message as well as any attachments.

Test your knowledge

- You receive a request to send PHI via fax to another medical facility as a referral for further treatment. There is a signed authorization from the receiving facility. You compile the information and send it via fax using a BR fax cover sheet.

- Two days later you received a call from the patient stating that the medical information was never received. Upon checking the request, you note that the fax number used was the wrong number and the medical information went somewhere else. You fax the information to the correct facility.

Test your knowledge

- What should you do next?
- You need to report the incident via the Verge system. If you have any questions regarding the incident, contact your Supervisor/Manager or the Privacy Officer at 4374.

Encryption

- BR policy concerning any PHI that leaves the facility electronically, it must be encrypted.
- More information is available at https://iconnect.brattlebororetreat.org/system/files/electronic_communication_policy.pdf

Test your knowledge

- You need to send information to a provider via email.
- What do you need to do to secure this information?
- You should ALWAYS send the message via the “Encrypt & Send” button located in the top left-hand corner of your email.

Managing Data

- Policies concerning data access are found at https://iconnect.brattlebororetreat.org/policies including use of mobile devices, laptops, smart phones, and any other portable device or media type.
- Access to BR client data is granted on an as needed basis and must be cleared appropriately.
- If you require access to client data using an offsite appliance, the management team will provide permission, technical support, training and guidance.
- Reporting of a possible HIPAA violation can be entered into Verge which is locate in IConnect under Applications

Test your knowledge

- Where can you access the policies and procedures that govern the protection of patient’s PHI and report any suspected HIPAA violations?

- Retreat policies are found on IConnect under the Icon labeled “Policies and Procedures.” The Verge reporting system can also be found in IConnect under Quick Links, Applications, Verge Event Reporting.

If you suspect a breach…

The Brattleboro Retreat has policies and procedures that assure the integrity, confidentiality and availability of PHI in order to operate our information systems.

All employees and contractors are responsible for reporting a possible or suspected breach of data security that comes to their attention.

Incidents should be documented immediately in a secure format (i.e., Verge) and reported to a Supervisor or to the Privacy Officer ext 4374.