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 in its common forms
- Know consumers rights under HIPPA
- Know how to safeguard PHI correctly
- How to comply with state and federal laws
- Understand the impact of potential violations

What is Privacy?

According to Merriam-Webster dictionary, the definition of privacy is:

The quality or state of being apart from company or

observation or freedom from unauthorized intrusion

<u>What does that mean for our patients?</u>

It means that everyone has the right to control access by other people to their personal and private information.

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

What are some examples of PHI?

Name, address, phone number, email address, social security number, medical record number, health plan number, account numbers, certificates and license numbers, device identifiers and serial numbers, web URLs, IP addresses, vehicle identifiers including license plates, biometric identifiers including finger prints, photographic information, and also information about relatives, household members and employers.

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

What is the big deal about PHI?

Protected Health Information is protected by Federal laws, including:

- HIPAA – the Health Insurance Portability and Accountability Act of 1996
- HITECH – the Health Information Technology for Economic and Clinical Health Act, which is a supplement to HIPAA 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

Why was HIPAA enacted?

- Laws at the local levels were inadequate and inconsistent
- To improve protection of private information
- To prevent disclosure of information in an inappropriate manner
- To require organizations to improve their systems that store, process or transmit private information, including the transition from paper to electronic medical records
- To establish nation-wide standards that improve patient record security and ultimately the health care industry

HIPAA has Rules

- The Breach Notification Rule following a breach
- The Enforcement Rule covers non-compliance
- 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

More about HITECH

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

- HITECH imposes civil penalties for willful neglect when protecting PHI, which increase for repeat or uncorrected violations. Audits are conducted regularly of organizations affected.
- In the event of a data breach, the Act requires that patients be notified. If the data breach involves a large number of patients, the US Department of Health and Human Services and possibly the local media also need to be notified.
- Compliance between business associates concerning HIPAA safeguards is required.

More about 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.

How is PHI stored or protected?

- Need to know means only the people who need access to a patient's information can access it, and then only the parts that affects their job.

- Physical and system safeguards are in place, such as locked doors, computer passwords, or preventing others from hearing conversations.

- Organizational policies and procedures for all methods of health information storage are to be in place and enforced per HIPAA regulations.

Why should I care?

Lots of reasons!

- It's the law – and breaking it could result in state and or federal prosecution resulting in fines or worse.
- It's policy – and breaking it can get you fired.
- There are procedures in place for conforming to these laws which you will learn as part of this course, in orientation and on your unit.
- How long do I need to follow PHI procedures? The short answer is forever. The long answer is also forever.

Remember: compliance with privacy laws and policies is very serious.

Rule: Need to Know

Is it 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, see if you can use identifiers that are not patient specific first.
3. If you still need PHI that is patient specific, be sure it is for the business at hand and is consistent with BR policies.
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.

Rule: 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

Rule: 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

Rule: Paper

- All paper documents that contain PHI must be filed and stored according to BR policy and procedure.
- 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.

Rule: Talking

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
- If PHI is been given out by mistake or incorrectly, talk to your supervisor
- Ways to contact your supervisor include telephone, email or in person.

Rule: 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. There should be no PHI in the subject line of the email.

Rule: 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

Rule: Managing Data

- Policies concerning data access are found at https://iconnect.brattlebororetreat.org/resources__help/policies_procedures 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.
- Audits are performed regularly in order to insure that PHI protections are adequate and compliant with state and federal laws.

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 and reported to a Supervisor or to the Privacy Officer.