WHAT IS HIPAA?

- HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996 (§45 C.F.R Parts 160 and 164).

- Provides a framework for the establishment of a nationwide protection of participant confidentiality, security of electronic systems, and standards and requirements for electronic transmissions of health information.

PARTS OF HIPAA

Privacy Rule

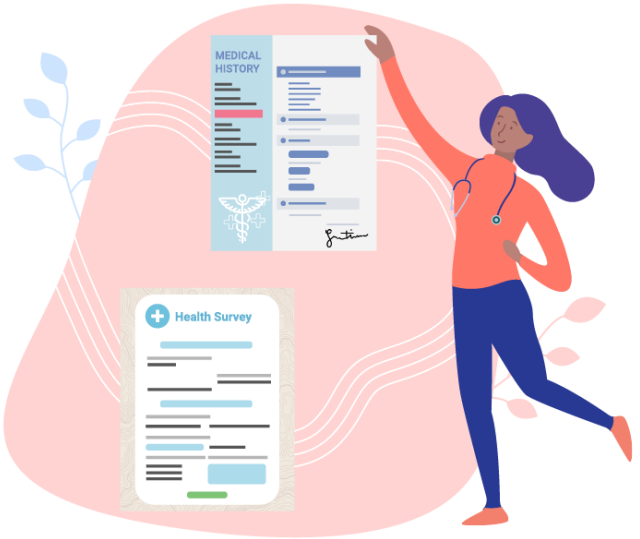
- The Privacy Regulations went into effect April 14, 2003.
- Privacy refers to the protection of an individual's health care data.
- Defines how participant information is used and disclosed.
- Describes how to properly share health-care info.
- Gives individuals privacy rights and greater control over their own health information.
- Outlines ways to safeguard Protected Health Information (PHI)

Security Rule

- Security regulations went into effect April 21, 2005.
- How to properly handle health-care information from improperly being viewed or altered (i.e. Beacon implemented the no personal cell phone policy on sight after a staff member had been taking pictures and sharing information with friends about a resident and staff.
- Security means controlling:
  - The confidentiality of electronic Protected Health Information (ePHI).
  - How consumer data is electronically stored.
  - How participant data is electronically accessed.

Electronic Data Exchange/Transfer Rule

- Standardizes certain types of communications between computers.



HIPAA REGULATIONS

The HIPAA Regulations require we protect our residents' PHI in all media including, but not limited to, PHI created, stored, or transmitted in/on the following media:

- Verbal discussions (Not using full names of residents in view of others, keeping private information private in conversation both internally and externally with only those who have a release signed for them.)
- Written on paper (Locking up their information.)
- In all of our computer applications/systems (i.e. NextStep, Clarity, etc.)
- In all of our computer hardware/equipment (Computer work for residents should not be done on personal computer.)

HIPAA DEFINITIONS

Protected Health Information (PHI)

Individually identifiable health information related to information about:

- Health/Condition of an individual
- Payment for health care of an individual
- Reasonably identifies the individual (consumer identifiers/demographics)
    - This includes information by which the identity of the resident can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information.

Examples of Consumer Identifiers

- Names
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification Numbers
- Vehicle Identifiers/Serial Numbers/License Plate Numbers
- Internet Protocol Addresses
- Health Plan Numbers
- Web Universal Resource Locators (URLs)
- Any dates related to individuals (date of birth)
- Telephone Numbers
- Fax Numbers
- Email Addresses
- Biometric identifiers including finger and voice prints
- Any other unique identifying number, characteristic or code
- Full face photographic images and any comparable images

MENTAL HEALTH CODE

However, the MI Mental Health Code has additional restrictions about the disclosure of patient information. Beacon is obligated to follow the Mental Health Code restrictions on disclosing resident information.

Mental Health Code Confidentiality (§330.1748 General Requirements and Considerations)

- Information in the record of a recipient shall be kept confidential
- Information may be disclosed outside of the holder of the record only with resident authorization or under specific circumstances
  - As necessary for the recipient to apply for or receive benefits
  - As necessary for the purpose of outside research, evaluation, accreditation, or statistical compilation. The individual who is the subject of the information shall not be identified in the disclosed information unless the identification is essential in order to achieve the purpose for which information is sought or if preventing the identification would clearly be impractical, but not if the subject of the information is likely to be harmed by the identification.
  - To a provider of mental or other health services or a public agency, if there is a compelling need for disclosure based upon a substantial probability of harm to the recipient or other individuals.

Why do we need to protect PHI?

- It is the law.
- To protect our reputation.
- To avoid potential withholding of federal Medicaid and Medicare funds.
- To build trust with our contracted providers and residents.

Who or what protects PHI?

- Federal Government through the HIPAA laws.
  - Civil penalties levels of monetary penalty amounts per violation.
    - $50,000 fine and 1-year prison for knowingly obtaining and wrongfully sharing information.
    - $100,000 fine and 5 years prison for obtaining and disclosing through false pretenses.
    - $250,000 fine and 10 years prison for obtaining and disclosing for commercial advantage, personal gain, or malicious harm.
- Beacon through our Privacy Practices.
- You by following our policies and procedures.

RESIDENT RIGHTS: ACCESS

Residents own their health-care information. The agency holding the information does not.

Residents have the right to inspect and copy PHI. However, there are some situations where access may be denied or delayed.

- Psychotherapy Notes
- PHI compiled for civil, criminal, or administrative action or proceedings
- A research study that previously secured agreement from the individual to deny access
- Access that is protected under the Federal Privacy Act
- PHI was obtained under the promise of confidentiality and access would reveal the source of the PHI

SECURITY RULE

Administrative Safeguards

Beacon policies and procedures must be followed by all staff to maintain security (i.e. disaster recovery of computer systems, use of the internet, use of email, faxing, use of voicemail, computer hardware and software standards).

Technical Safeguards

Many technical devices are needed to maintain security. Examples include varying levels of passwords, screen savers, data backups, disposal of media, encryption, and audit trails. Computer and system processes are set up to protect, control, and monitor information access.

SECURITY RULE

Physical Safeguards

Many physical barriers and devices are needed to maintain security. Examples include installing locks on doors, securing buildings and rooms, and identifying visitors.

Personnel Security

Beacon policies and procedures manage the assignment of access authority to employees. Procedures should address employee transfers, role changes, and terminations. Effective security and privacy training must be conducted.

ePHI Access

Usernames and Passwords

How do we control access to electronic Protected Health Information (ePHI) in our computer systems?

- By requiring all users to utilize individually unique usernames and passwords, we control access to the information.
- Usernames and passwords control what users can access and help us identify what information users accessed in our applications.

For this reason, you **SHOULD NOT** share usernames and passwords with anyone else.

How to Protect Your Logins

- Memorize your passwords. Don't post usernames and passwords on your computer, notebook, tablet, under your keyboard, in an unlocked drawer, etc.
  - Secure any written usernames and passwords in a locked location to prevent access to them by someone else.
- If you believe one of your usernames and passwords have been compromised, request that it be changed.
  - If you think PHI may have been inappropriately accessed, discuss your concerns.

RELEASE OF INFORMATION: IDENTITY VERIFICATION

HIPAA privacy regulations do not apply to discussing medical information with family members. This gets tricky with our residents. If a release of information has been obtained for family members (or they are guardian), information can be shared.

Prior to releasing PHI, ask the individual to provide you with enough information to identify the consumer, such as:

- Name
- Address
- Date of Birth
- Other identifiers like social security number, mother's maiden name, etc.

Identify someone other than the resident by requesting they provide you with all the above information, as well as their relationship to the resident.

Once you know who the requestor is, be sure they have been included in the Release of Information for the resident.

Provide only the minimum necessary information to safeguard PHI.

VIOLATIONS

Incidental Violations

If reasonable steps are taken to safeguard a resident's info and someone happens to overhear or see PHI. There is typically no liability.

An incidental disclosure is not a privacy incident. This type of disclosure is not required to be documented.

Accidental Violations

If you mistakenly disclose PHI or provide confidential info to an unauthorized person or if you breach the security of confidential data.

1. Acknowledge the mistake and notify your supervisor immediately.
2. Assist in correcting the error only as requested by supervisor or Compliance. Don't cover up or try to make it "right" by yourself.

Accidental disclosures are Privacy Incidents and must be reported immediately. We are required to document this type of disclosure.

Intentional Violations

If you ignore the rules and deliberately or carelessly use or disclose protected health or confidential info, you can expect:

1. Disciplinary action, up to and including termination
2. Civil and/or criminal charges

Examples include accessing PHI for purposes other than your assigned job responsibilities or attempting to learn or use another person's access information.

HIPAA HITECH, FEBRUARY 2010

1. Violations of HIPAA now include penalties for individual employees as well as employers. The fines went from $25,000 to as much as $1.5 million for "willful neglect".
2. If a violation has occurred, it must be disclosed not only to consumers, but also to HHS; and in some cases, to the media no later than 60 days after the discovery of the breach.
3. HITECH stands for Health Information Technology for Economic and Clinical Health Act. It includes the necessity for "encryption" (security measures like passwords, etc.) for all data sent or received electronically.
4. Workers' comp injuries are not protected by HIPAA; however, most companies are now encouraged to protect this information to the best of their ability.