# Health Insurance Portability and Accountability Act (HIPAA)

BEACON
Specialized Living

# Course Objectives

BEACON Specialized Living

Build your understanding of the Health Insurance Portability and Accountability Act (HIPAA) and HITECH.

Understand your rights and responsibilities in maintaining the confidentiality and security of Protected Health Information (PHI) of your Residents.

Outline the consequences for your Resident, Beacon, and for yourself if the Act is violated and how to report a violation.

How Informed Consent, Confidentiality, and HIPAA work with one another.

Learn when to release confidential information in compliance with HIPAA standards depending on the situation.

Learn your HIPAA resources.

# What is HIPAA?

BEACON Specialized Living

- HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996 (§45 C.F.R Parts 160 and 164).
- It is a Federal Law that 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.
- Applies to any staff that handles a Resident's protected health information (PHI), provides care to the Residents, or works in areas where such information could potentially be heard.
- Requires that staff do not have access to view PHI unless there is a proper reason.

# Why is HIPAA needed?

BEACON Specialized Living

- Sets the security standards for the healthcare industry that were not previously outlined.
- Allows the healthcare industry to ensure security among the evolution of new digital technology while phasing out hardcopy records.
- Combat healthcare fraud and abuse.
- Define Covered Entities.
  - The organizations who are required to follow HIPAA. These are providers who electronically transmit any health information in connection with transactions.

# Parts of HIPAA

BEACON Specialized Living

## Privacy Rule

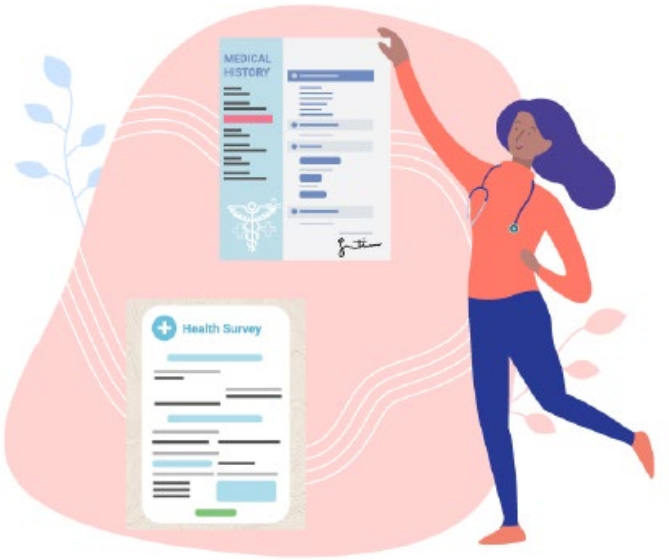
- The Privacy Regulations went into effect April 14, 2003.
- Privacy refers to the protection of an individual's health care data.
- Defines how participant information is used and disclosed by covered entities.
- Describes how to properly share health care info.
- Gives individuals privacy rights and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

## Security Rule

- Security regulations went into effect April 21, 2005.
- Refers to how to properly handle healthcare information so it cannot be improperly 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 (keeping secret/private) 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.



BEACON
Specialized Living

# Privacy Rule Spotlight

## Confidentiality

Resident's PHI is confidential. This means that their information cannot be shared without their prior written permission or as required by law. At Beacon, we have the duty to take reasonable steps to keep their PHI confidentiality consistent with their preferences. This may mean not allowing a well-meaning family member to have information about them if they do not want it.

All Residents are entitled to confidentiality unless they give permission for disclosure.

## Minimum Necessary Rule

Staff are limited in the amount of PHI they can interact with based on what services they provide. They will only be able to access the minimum amount of PHI information they need to fulfill the duties.

This allows the minimum amount of PHI to be shared and safeguard the confidentiality of Resident's PHI. It also lowers the chances of PHI being released when it is not necessary for services.

An example is that Direct Care staff do not have access to billing information because it is not necessary for the care they provide. While the billers will have access to that information but not the resident's Daily Care Log.

BEACON Specialized Living

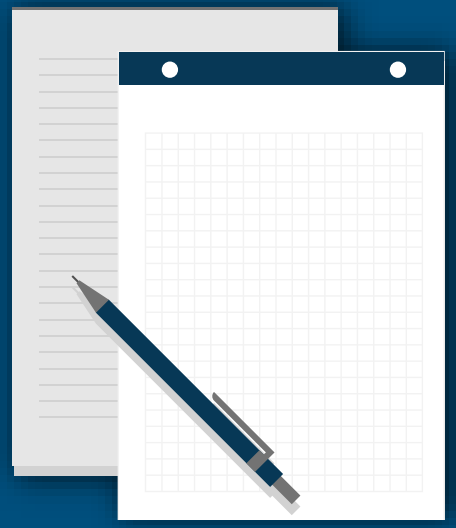
# Privacy Rule Spotlight

## Informed Consent

Informed consent means not only that a Resident (or legal guardian, if applicable) can discuss and agree (or not agree) to release information about themselves or the services they are receiving. It also means that the person receiving services gives a release voluntarily, with the full understanding and knowledge of what the release means, It means that:

- The Resident (or legal guardian, if applicable) is not pressured in any way to give consent.
- The Resident (or legal guardian, if applicable) is able to understand what they are agreeing to release.
- The Resident (or legal guardian, if applicable) understands the risks, benefits, and consequences of agreeing, or not agreeing, to approve the release of information about themselves or the services they are receiving.

Informed consent must be given by the Resident (or legal guardian, if applicable) when they agree to have information about their treatment released to persons or entities outside Beacon. A person who has a guardian is not capable of giving informed consent.




BEACON
Specialized Living

# Privacy Rule Spotlight

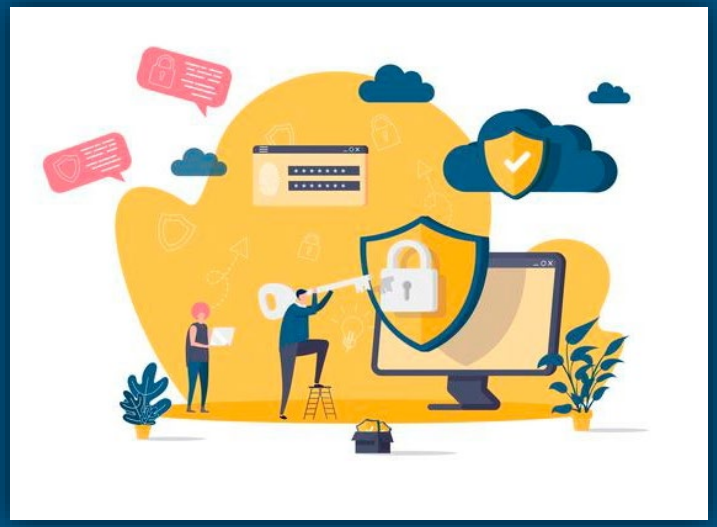
## Use vs Disclosure

Use means with respect to PHI, the sharing, employment, application, utilization, examination, or analysis.

*Example: accessing the eMAR for a resident.*

Disclosure means the release, transfer, access to, or divulging in any other manner of information outside the entity holding the information.

*Example: Sharing information about a resident with their family or friends.*



BEACON
Specialized Living

# Security Rule Spotlight

## Administrative Safeguards

Beacon policies and procedures must be followed by all staff to maintain security. Beacon's policies can be found on the Employee Basecamp on the Policies and Forms page. These policies include, but are not limited to

- Disaster Recovery of Computer Systems
- Use of the internet
- Use of Email and faxing
- Use of Voicemail
- Computer Hardware and Software standards

See the Reference Slide for specific Policy numbers for more information.

## 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.

BEACON
Specialized Living

# Security Rule Spotlight

## Physical Safeguards

Many physical barriers and devices are needed to maintain security. Examples include

- Installing Locks on Doors
- Securing Buildings and Rooms
- Identifying Visitors

## Personal Security

Beacon's policies and procedures manage the assignment of access authority to employees. HR and Supervisors will follow the proper procedure when carrying out

- Employee Transfers
- Role Changes
- Terminations

# Protected Health Information

Is health-related information that is transmitted electronically, orally, or written and can be reasonably used to identify a Resident. They can be related to:

- Health or Condition of an individual.
- Payment for health care of an individual.
- Reasonably identifies the individual. Also known as Consumer Identifiers or 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.

BEACON
Specialized Living

# Examples of Unique Identifiers

- Names
- Geographic Demographic
- URLs
- Health Status (Diagnosis, Records)
- Provision of Care (Services Received)
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License or Certification Numbers
- Vehicle Identifiers/Serial Numbers/License Plate Numbers
- Internet Protocol Addresses
- Billing Information
- Any dates related to individuals (i.e. Birth Date, Discharge Date, etc.)
- Telephone & Fax Numbers
- Past/Present/Future Physical or Mental care
- Postal and Email Addresses
- Biometric identifiers including finger and voice prints
- Full face photographic images and other comparable images
- Any other unique identifying number, characteristic or code

BEACON
Specialized Living

# Protecting PHI

BEACON Specialized Living

## 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 Penalty levels of monetary amounts per violation.
    - $50,000 fine and 1-year prison sentence for knowingly obtaining and wrongfully sharing information.
    - $100,000 fine and 5-year prison sentence for obtaining and disclosing through false pretenses.
    - $250,000 fine and 10-year prison sentence for obtaining and disclosing for commercial advantage, personal gain, or malicious harm.
- Beacon and you through our Privacy Practices and practicing confidentiality.
  - Do not alter or destroy PHI.
  - Ensure that PHI is available for use for an authorized person(s).
  - See the list of References at the end of the presentation for specific Policy Numbers relating to HIPAA and PHI at Beacon.

# HIPAA HITECH

HITECH stands for Health Information Technology for Economic and Clinical Health Care Act and went into effect February 2010. The final form went into effect in 2013. It widen the scope of HIPAA to the digital platforms and outlined standardized security for emerging technology in response to the popularization of electronic recordkeeping and communication.

- Focuses on electronic health records (ePHI).
- Outlines the impact on PHI by the emergence and evolution of data mining and collection services and applications as agencies are encouraged to use electronic health records.
- Increased the potential liability for non-compliance. Violations of HIPAA will 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”.
- If a violation has occurred, it must be disclosed not only to Residents but also to HHS; and in some cases, to the media no later than 60 days after the discovery of the breach.
- Workers’ comp injuries are not protected by HIPAA; however, most companies are now encouraged to protect this information to the best of their ability.

BEACON
Specialized Living

# ePHI Access

BEACON Specialized Living

## 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.
  - Do not post usernames and passwords on your computer, notebook, tablet, under your keyboards, 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 logins have been compromised, request it has changed.
  - If you think PHI may have been inappropriately accessed, discuss it with the Compliance Department and your supervisor ASAP.

# Mental Health Code

The MI Mental Health Code has additional restrictions on the disclosure of patient 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 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 the substantial probability of harm to the recipient or other individuals.

BEACON
Specialized Living

# Resident's Rights to Access

Residents own their healthcare 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; and
- PHI was obtained under the promise of confidentiality and access would reveal the source of the PHI.

BEACON
Specialized Living

# HIPAA and You

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

## Verbal Discussions

- Do not use full names of residents in earshot of others.
- Keep private information private in conversations both internally and externally.
- Only share information with those who we have a signed release for.

## Written on Paper

- Do not leave papers out in the open. Lock up paperwork when not in use.
- Do not just throw information away in an accessible trash can. All sensitive documents should be put in the designated locked disposal.

## Computer Applications & Hardware

- This includes NextStep, Clarity, etc.
- Do not access in public spaces.
- Do not stay logged into the account when you are done. Lock your computer when you step away from the desk.
- Computer work for residents should not be done on your personal computer.

BEACON Specialized Living

# Resident information can only be disclosed when...

1. When the resident (or legal guardian) agrees and the person requesting the information provides a legitimate need for the information.
2. To Mental Health or other public agencies when there is a strong chance that the Resident or others will be seriously harmed if no action is taken.
3. Without a Resident (or legal guardian's consent) information can only be given to the provider of mental health services when the information is necessary for the provision of care, treatment, and/or services.
4. As necessary to agencies like Social Security Administration or Family Independence Agency for various services.
5. By court order, or when necessary to comply with law.
6. To a prosecuting attorney when necessary for him/her/they to participate in proceedings governed by the Mental Health Code.
7. To a prosecuting attorney to allow the recipient to participate in proceedings governed by the Mental Health Code.
8. To the Resident's attorney when the Resident (or legal guardian, if applicable) has given consent.
9. To the Office of the Attorney General.
10. For research or accreditation, and only when the Resident will not be harmed by the disclosre, and the identity of the Resident can be protected.
11. To a surviving spouse. If there is no spouse, then to the Resident's closest relative so those individuals can apply for and receive benefits.

BEACON
Specialized Living

# Release of Information: Identity Verification

HIPAA privacy regulations doesn't apply to discussing medical information if a release of information has been obtained for a Resident's family members (or if they are a guardian). Do not let anyone pressure you. Your first responsibility is to guard Resident Rights concerning confidentiality. First, you want to identify and verify the resident whose information they're requesting.

To do this, ask the individual to provide you with enough information to identify the Resident, such as:

- **Name**
- **Address**
- **Date of Birth**
- **Other Identifiers like Social Security Numbers, Mother's maiden name, etc.**

BEACON
Specialized Living

# Release of Information: Identity Verification

To verify the requestor's identity, request they provide you with the same information, as well as their relationship to the resident.

- **Name (and entity name if applicable)**
- **Address**
- **Date of Birth**
- **Other Identifiers like Social Security Numbers, Mother's maiden name, etc.**

Once you have confirmed who the requestor is, be sure that they have been included in the Release of Information Form for the Resident.

- Ask your supervisor about who is authorized or ask to see the authorization that the Resident (or designated representative, if applicable) has signed specifying what information can be released to whom. If they are not, explain that you cannot provide the requested information.
- When in doubt, refer them or the entity they represent to your supervisor.

**Remember!** Provide only the minimum necessary information to fulfill the request to ensure PHI is safeguarded.

BEACON
Specialized Living

# Consent to Share Behavioral Health Information Form

This is the MDHHS required release of information form. It was developed as a standard release form for exchanging confidential mental health and substance use disorder information for use by all public and private agencies, departments, corporations, or individuals that are involved with treatment of an individual.

It can be found in a Resident's NextStep forms and is completed upon intake.

BEACON
Specialized Living

# Violations

## Incidental Violations

Reasonable steps were 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

You mistakenly disclose PHI or provide confidential info to an unauthorized person, or 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

You ignore the rules and deliberately or carelessly use of 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.

BEACON Specialized Living

# Resources:

Health Information Privacy at HHS.gov

Health Insurance Portability and Accountability Act of 1996 (§45 C.F.R Parts 160 and 164)

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

Michigan Mental Health Code Behavioral Health Information Sharing and Privacy

## Beacon Policies

[HIPAA-001] HIPAA and HITECH

[HIPAA-002] Notice of Information Practices

[HR-038] Personnel Security

[HR-046] Cellular Phones

[IM-010] Breach Notification – Protected Health Information

[LD-008] Corporate Compliance Plan

[CTS-004] Confidentiality, Abuse, Neglect & Mandatory Reporting Requirements

## Beacon Tell Me How Guides

[MED.TMH-008] Medical Appointments

[CTS-004] Confidentiality, Abuse, Neglect & Mandatory Reporting

BEACON
Specialized Living