HIPAA stands for:

a. Health Inclusion Portability and Assurance Act  
b. Health Information Protection and Assurances Act  
c. Health Identification Protection and Accountability Act  
d. Health Insurance Portability and Accountability Act

2. What did the 2013 Omnibus Privacy, Security, Enforcement, and Breach Notification Rule do regarding HIPAA information?

a. Made effective the original HIPAA legislation  
b. Introduced the definition and criteria for protected health information (PHI)  
c. Implemented HITECH Act provisions, which expand HIPAA protections and fines for noncompliance  
d. Limited the power of state and local authorities to enforce privacy and security protections for patient data

3. ______ prevents someone from hearing or seeing a person’s private health records and information unless he or she has the proper permissions.

a. Privacy  
b. Confidentiality  
c. Security  
d. None of the above

4. Which of the following is NOT an example of PHI?

a. Resident record  
b. Favorite color  
c. Date of birth  
d. Employer

5. A facility must always allow a resident to view and photocopy his or her PHI if that person submits a request, even if doing so could put the resident’s health at risk.

a. True  
b. False

6. Under HIPAA, if a facility wants to disclose a resident’s PHI for a purpose other than providing healthcare, it is required to obtain that individual’s ________.

a. electronic health record  
b. consent  
c. authorization  
d. None of the above

7. To comply with HIPAA, skilled nursing facilities and other covered entities are required to do all of the following EXCEPT:

a. Notify residents of their privacy rights  
b. Burn all old files  
c. Train employees so that they are fully aware of privacy procedures  
d. Implement safeguards to prevent misuse of PHI

8. A cover sheet marked “Confidential” should accompany all faxed information pertaining to residents.

a. True  
b. False

9. When emailing information about a resident, staff should

a. avoid using any detailed identifying information  
b. use a computer that many visitors can see and access  
c. use casual language and abbreviations wherever possible  
d. refer to the resident by his or her full name

10. Even if frontline staff are certain that the person they are speaking with is permitted to hear certain information, they should not discuss a resident’s PHI ________.

a. on Facebook  
b. at parties  
c. in restrooms of public buildings  
d. All of the above


**HIPAA: SAFEGUARD RESIDENTS’ PHI**

Congress passed HIPAA to safeguard the privacy, confidentiality, and security of every person’s health information. For those in the long-term care industry, these expectations should translate to honoring residents’ specific rights under the legislation when providing care.

Residents have the right to:

- **Privacy**, which dictates who should and should not have access to their protected health information (PHI). This information should only be available to people who need it to provide care.
- **Confidentiality**, which prevents people from hearing or seeing an individual’s private health records and information unless they have the appropriate permissions. Because all PHI is confidential, anyone who accesses it is responsible for its protection.
- **Security**, which is the vehicle for providing privacy and confidentiality. Its purpose is to ensure that PHI is accessed only by authorized individuals.

Providing quality resident care requires communication between workers from different disciplines and settings. Today’s plethora of electronic mediums makes sharing important information about residents easier than ever. However, this convenience also means that confidentiality is often readily available to anyone who walks by a fax machine or logs on to a computer—a vulnerability that can be particularly disquieting for people who fear that the exposure of their PHI could result in job discrimination, embarrassment, or the loss or denial of health insurance.

Therefore, with the growing presence of electronic data, which increasingly replaces or supplements paper files, providers and staff must make sure they’re equipped to protect health information in any form. Federal laws, such as HIPAA, help accomplish this by ensuring every state and healthcare organization follows the same rules for promoting privacy, confidentiality, and security.

**HIPAA coverage and expectations**

The privacy protections of HIPAA apply to PHI, which is information that:

- Is created or received by a covered entity or an employer that relates to a person’s past, present, or future health condition, health treatment, or payment for healthcare services
- Could identify an individual, such as name, address, telephone number, date of birth, diagnosis, medical record number, Social Security number, employer, or position
HIPAA: SAFEGUARD RESIDENTS’ PHI

PHI can come in any format (paper, electronic, or oral). The most common example of PHI is the resident record.

The following public and private organizations are considered covered entities under HIPAA and must therefore comply with its provisions for protecting PHI:

- Health plans and health insurance companies, such as health maintenance organizations and preferred provider organizations
- Healthcare clearinghouses, such as billing services
- Healthcare providers of any type or size, including doctors, dentists, therapists, hospitals, clinics, pharmacies, home health agencies, hospices, and long-term care or personal care facilities

These entities are required to communicate details of HIPAA to both patients and frontline staff. For long-term care providers, this process should include:

- Notifying residents about their privacy rights and offering clear written explanations of how the facility may use and disclose their health information. This explanation, often called a privacy notice, must inform residents of their right to view their own records, obtain copies of those records, have copies sent to another person or organization, request restrictions on how their PHI is used and disclosed, receive confidential communications and a report of certain disclosures of their PHI, and request amendments to their information. The notice must also inform residents about how to file a complaint with the facility or the Office for Civil Rights.
- Writing, implementing, and educating employees on privacy procedures that define who has access to protected information, how the facility will use the information, and when the facility might disclose the information to others.
- Appointing an individual to ensure that employees follow privacy procedures, and installing other safeguards to prevent any misuse of PHI.
- Recording instances where the facility has disclosed PHI for purposes other than treatment, payment, or healthcare operations.

Covered entities are required to have a sanctions policy in place for disciplining employees and other workforce members who violate HIPAA’s Privacy, Security, or Breach Notification Rules—an important requirement to comply with since such actions can result in civil or criminal penalties for an individual or group of individuals, as well as severe consequences for the organization.

Protecting residents' records

Although the HIPAA Privacy Rule specifies that obtaining a patient’s consent is optional when a covered entity discloses PHI to another party for treatment, payment, and healthcare operations (e.g., a resident’s doctor shares PHI with a second doctor who can provide valuable input on care strategies), some facilities may choose to implement policies that require this additional safeguard. These expectations may direct the resident to sign a consent form prior to disclosure, though the HIPAA Privacy Rule states that the specifics of this process are at the discretion of the covered entity.

However, there is much less flexibility if a facility wants to disclose a resident’s PHI for a purpose other than providing care. In such cases, the facility needs that person’s specific authorization. To grant these specific permissions, a resident must sign an authorization form before each individual instance of disclosure.

In addition to gaining appropriate permissions before sharing residents’ health information with other parties, a facility must also allow residents to view and photocopy their PHI if they submit a request. However, there are a few special circumstances under which a facility may not need to grant a resident access to his or her PHI, such as when:

- The facility compiled information for use in a civil, criminal, or administrative proceeding
- There is reason to believe that access to PHI might put the resident’s health at risk
**HIPAA: Safeguard Residents’ PHI**

In addition, if a resident believes that his or her PHI contains information that is incorrect, he or she may ask the facility to make changes. Facility leadership may deny the request if they believe the current information is accurate and complete, or if the information was not captured by the facility.

**Mobile and online considerations**

Only authorized personnel should enter confidential medical information into a computer-based resident record. Computer systems should be password-protected to help guard against unauthorized access and use.

In addition, all LTC staff should exercise discretion and vigilance when using technologies on the job to help protect resident information. This includes properly managing electronic passwords, preventing the spread of viruses, logging off the computer, protecting tablets and smartphones (if used for care), and being cognizant of any resident information taken or accessed off-site, as well as the implications of these actions.

As key frontline staff members, CNAs should know and understand their facility’s policies on which devices can be used for work and in what manner. Remember that HIPAA applies to all communication, including the entire spectrum of social media. In other words, Facebook, Twitter, LinkedIn, Instagram, text messages, etc., are not appropriate avenues for sharing any kind of resident information. No matter how innocuous a post or text may seem, if it reveals a resident’s PHI in any way, staff could find themselves in serious trouble.

**Exceptions to the HIPAA Privacy Rule**

Clearly, HIPAA includes stringent provisions to safeguard residents’ privacy. However, under certain state and local laws, the HIPAA Privacy Rule directs covered entities to disclose an individual’s healthcare information without his or her specific authorization for special reasons, including:

- Emergencies
- Public health needs (e.g., infectious disease registries)
- Mandatory reporting of child or elder abuse and neglect
- Judicial and administrative proceedings
- Substantial communication barriers

If there is no state or local law specifically requiring disclosure of information in the instances listed above, covered entities are required to use “professional judgment” in deciding whether to disclose information and how much to disclose.

**Top HIPAA action items for frontline staff**

- Consider it a top priority to keep all protected health information (PHI) confidential, regardless of its form. Do not leave resident records open where unauthorized persons can see them, and discuss any resident information in a private place so others cannot overhear the conversation.
- Ensure residents understand their right to decide and be made aware of who may have access to their health information and under what circumstances.
- Do not share information you learn on the job with a resident’s family or friends. Always obtain residents’ permission before sharing PHI with these individuals.
- Learn the safeguards your facility requires for the use, disclosure, and storage of PHI, as well as your facility’s specific privacy policies and procedures.
- Only enter confidential medical information into a computer-based resident record if you are authorized to do so.
- When emailing information about a resident, avoid using any detailed identifying information. For example, refer to the resident by initials or an internal resident number instead of by his or her full name.
- Include a cover sheet labeled “Confidential” with all faxed information.
- Use objective, precise language when documenting in the resident record. Avoid casual remarks and abbreviations that could be misunderstood.