e-Compliance Training

HIPAA Privacy Rule - April 2019

THIS TRAINING SESSION IS RECOMMENDED FOR:

All workforce members that have access to patient information. HIPAA regulations use the term *workforce member* instead of *employee*. Workforce members include providers, employees, volunteers, interns, students, trainees, etc.—anyone who will be granted access to your patient's protected health information (PHI), and who will be working under the control of the practice.

Training Objectives

The objectives of this training module are to provide awareness and understanding of:

- Privacy Rule definitions and standards;
- Responsibilities for accessing, using and disclosing PHI; and
- Rights afforded to patients.

Table of Contents

Background

The Privacy Rule is one standard within the HIPAA regulations, and is intended to protect the privacy of individually identifiable protected heath information (PHI) in any form—meaning that Privacy Rule requirements apply to verbal, written, and electronic information. Other standards address electronic transactions, security of electronic information, enforcement and breach notification.

Definitions

Several Privacy Rule definitions will help to ensure that you understand specific requirements.

Individual - The term *individual* means a patient or other person who is the subject of the information being collected/maintained/used/disclosed. Sometimes, your practice might receive information on an individual who has not yet become a patient. The rights of the Privacy Rule apply to an individual whose information you may have collected, whether or not they are considered a patient of your practice.

Protected Health Information (PHI) - PHI is any information that identifies an individual and describes his/her health status, sex, age, ethnicity, billing or demographic characteristics. All of the information maintained in a patient's medical or dental record is considered to be PHI. This applies even if you store clinical information in one place, such as an EHR, and billing and scheduling information elsewhere, such as in practice management software. All of the collective information is considered PHI.

Use – Health information that is maintained by the practice is "used" when workforce members access it to perform their job duties or share it with each other, but the information stays **within** the organization.

Disclosure – "Disclosure" of PHI occurs when it is shared with persons and entities outside of your organization. There are many instances in which disclosure does not require patient authorization. Examples of permitted disclosures not requiring patient authorization include disclosures for treatment, payment, and healthcare operations to other providers, pharmacies, insurance companies, healthcare clearinghouses, health plans, collection agencies, etc.

Interactive Training Reminder

Compliance Training is an interactive training program in which you can address questions with other staff members or supervisors to obtain clarification for situations in your work setting.

Write down any questions that you have about the training topic and address them with your Training Coordinator or supervisor.

Other Permitted Disclosures - There are other permitted disclosures, such as to law enforcement, public health, military services, for communicable diseases, in cases of abuse or neglect, for legal proceedings, to the Food and Drug Administration, to coroners, funeral director, and organ donation organizations, for military activity and national security, for worker's compensation, when the patient is an inmate, and in cases of criminal activity (which do not require a patient's authorization if certain conditions are met). Your Privacy Officer or other designated person will usually handle such disclosures to ensure Privacy Rule requirements are met.

Some disclosures **will** require patient authorization, such as disclosure of health information to individuals or entities (i.e., family members, friends or other individuals, life insurance companies, or other third parties) identified by the patient. Check with your Privacy Officer on the process for disclosures.

Certain limited disclosures to friends and family may be made without a written authorization. Examples include limited disclosures to a care giver who is helping a patient understand a medication or treatment plan, limited disclosures to persons involved in paying for a person's care, etc. If a friend or family member wishes to receive more detailed information on a patient, or a copy of the patient's record, an authorization should be obtained.

Treatment, Payment and Healthcare Operations – This phrase defines how a patient's PHI may be used or disclosed by your practice for the purpose or process of providing treatment, obtaining payment for treatment, or other necessary uses and disclosures which affect the operation of your practice. Some examples of activities covered by healthcare operations include: reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities.

Workforce Member Responsibilities

All workforce members must receive HIPAA training upon hire and annually thereafter, and must follow established privacy policies and procedures. The overall privacy responsibilities for workforce members include:

Minimum Necessary Standard- You will only access PHI necessary for the performance of your assigned duties. This means that you will not access a friend, family member, athlete or celebrity's record unless you have a work reason to do so. Even if you are a patient of the practice, you should request access in the same way as a normal patient would, and not enter your own record unless your job duties require it. In general, you will only disclose the minimum amount of information necessary for the stated purpose. Disclosures made for treatment purposes, to the individual who is the subject of the information, that are required by law or made pursuant to an authorization are exempt from minimum necessary requirements.

Acting as authorized- You will not divulge, copy, release, sell, loan, review, alter or destroy any confidential information, except as properly authorized by and relative to your responsibilities within the practice.

Safeguards - You will not misuse or act carelessly with PHI. You will safeguard and not divulge information that could provide unauthorized persons with access to PHI. Reasonable safeguards include being aware of the environment when making phone calls or having discussions with other staff members or patients regarding PHI. Speaking in a lower than normal volume or moving to a more private area to limit others from overhearing is considered a reasonable safeguard. Likewise, reasonable safeguards should be observed when leaving phone messages for patients. For example, only leave the name of the practice, a contact person and phone number for the patient to return the call. When faxing PHI, verify the fax number of the intended recipient. And finally, when emailing PHI, ensure that the message is encrypted, or if the patient requested PHI via email, that he/she has accepted the risk of interception. It is best to get such requests in writing to prevent privacy complaints. The same identity verification methods used for faxing should be used to ensure email messages are sent to intended recipients.

Incidental disclosures, such as a patient overhearing another patient's name, or a brief snippet of a conversation are not violations of the Privacy Rule, as long as reasonable safeguards are in place. You should always adhere to the safeguards that your practice has established to protect patient privacy.

Reporting Risks – You are responsible to report to the practice's Privacy Officer any activity that you suspect may compromise the confidentiality of PHI.

Personal Liability - Your obligation to maintain the confidentiality of protected health information that you have accessed/used continues even beyond your term of employment/association. You could be held personally liable for damage to a patient if you deliberately misuse information, or provide another person/entity with the means to do so.

Privacy Responsibilities

Acknowledgement of Receipt - Entities make a "good faith effort" to obtain a signature or initials from a patient acknowledging that they've received a copy of the Notice of Privacy Practices (NPP). While written acknowledgement is recommended, the Privacy Rule allows a practice to proceed without it. If a patient refuses to acknowledge receipt of the Notice, a practice can make a notation in the patient's chart of the refusal, the perceived reason for refusal, the "good faith effort" that was made, and proceed with treating that patient.

Business Associate Agreements - A Business Associate is a person or entity to which the practice will intentionally disclose PHI and, using that PHI, the business associate will provide a service to/for the practice. Examples of business associates include healthcare clearinghouses that handle billing information, transcription services, answering services, shredding services, cloud-hosting providers, IT vendors, collection agencies, mailing services, etc. A business associate agreement requires the business associate to comply with HIPAA requirements to protect the confidentiality of PHI they receive/access.

Refraining from Intimidating or Retaliatory Acts – Practices must implement policies and procedures that will prevent any retaliation or intimidating act against an

individual that exercises his/her rights under the Privacy Rule, including filing a complaint against your practice. As a workforce member, you should be aware of this requirement, and then ensure that your conduct never threatens a patient with retaliation or intimidation. You would also report to your Privacy Officer if you witness retaliation/intimidation against a patient exercising his/her rights.

Sanctions - The Privacy and Security Rules require a practice to establish sanctions/disciplinary action that would be imposed whenever there is a failure to follow the privacy and security policies and procedures of the practice. As a workforce member, failure to comply with Privacy or Security Rule requirements could result in sanctions, loss of employment and/or personal legal liability for you, depending upon the nature of the incident.

Confidentiality Statement – Your practice may require you to sign a confidentiality statement that acknowledges your understanding of the requirements for maintaining PHI in a confidential manner. Your practice may periodically ask you to review the statement and sign a new copy to confirm your continued understanding of your responsibilities, which extend beyond employment/association.

Patient Privacy Rights

Receive Notice of Privacy Practices – Individuals have the right to receive a Notice of Privacy Practices that includes a list of the patient's rights, the responsibilities of the practice and a description of how the practice will use and disclose PHI. The Notice must include a contact to which the patient may communicate a privacy complaint (i.e., the practice's Privacy Officer or the Office for Civil Rights (OCR)). Now is a good time for you to review your practice's Notice so that you are familiar with its content. Contact your Privacy Officer if you have questions.

Right to authorize other uses and disclosures - Patients have the right to authorize any use or disclosure of PHI that is not specified within your practice's Notice. For example, you would need a patient's written authorization to use or disclose PHI for marketing purposes, for most uses or disclosures of psychotherapy notes, or to sell PHI.

Alternative/confidential communication – Patients have the right to ask you, in writing, to contact them using an alternative method (i.e., email, telephone), and to a destination (i.e., cell phone number, alternative address, etc.) designated by them.

Right of Access - Patients may inspect and obtain a copy of their complete record. This includes all demographic, billing and clinical information that your practice has created, collected or maintains, with very few exceptions. This right to access and obtain copies includes all information that your practice has collected from other sources (i.e., other providers). If patient records are maintained electronically, a patient will also have the right to request a copy in electronic format. Patients also have the right (with few exceptions) to review original records under supervision. The Office for Civil Rights (OCR) has emphasized that any fee for records must be strictly based on actual cost and must be reasonable. You may not withhold a patient's information for a past due balance, but may require payment of the medical records fee prior to release. The OCR has also emphasized that practices may not impose unreasonable measures that inhibit a

patient's right of access. For example, you may not require a patient to come on site to request a copy of their record, but must allow them to make a remote request, if desired. The practice can verify the identity of the patient without requiring the patient to come into the practice.

Right to Designate a Personal Representative - A patient has the right to designate a personal representative who will be given the authority to authorize the use or disclosure of PHI on the patient's behalf. In the case of a minor child, parents and legal guardians are automatically considered a personal representative, and have the right to access the minor's information, with few exceptions.

Restrictions of PHI – Patients may ask, in writing, that your practice not use or disclose any part of their protected health information for the purposes of treatment, payment or healthcare operations. You have the right to agree to or deny regular restriction requests. There is one type of restriction request that you may not deny. Patients have the right to request, in writing, that a practice restrict communication to health plans regarding a specific treatment or service that the patient, or someone on his/her behalf, has paid for in full, out-of-pocket. This type of restriction request may not be denied, but full payment may be required up front.

Amendments to PHI - Patients may ask the practice to add a note or amendment to an item in their medical record, if they feel information is inaccurate. While the original record cannot be changed, an amendment can be added to a record noting the individual's request. The practice has the right to agree to or deny such requests. If your practice agrees to the requested amendment, it must become part of the individual's record. If the practice denies the patient's request, the patient has the right to disagree with your denial and submit a written disagreement that will become part of the medical record. Your practice can choose to write a rebuttal to the disagreement and that, again, will become part of the patient's record.

Disclosure accountability - This means that patients may request a listing of disclosures that your practice has made, of PHI, to entities or persons outside of the practice for purposes other than for treatment, payment or healthcare operations.

Notice of privacy breach - Patients have the right to receive written notification if your practice discovers a breach of unsecured PHI and determines through a risk assessment that notification is required. HHS must also be notified of any confirmed privacy breach. The key term is "unsecured PHI." PHI is only considered secure if it is unusable, unreadable, or indecipherable to unauthorized individuals.

Examples of breaches of PHI would include a lost or stolen device (i.e., computer, smart phone, flash drive, etc.) that stores unsecured patient information. A lost chart or other printed material containing PHI would also be considered a potential breach, because you cannot encrypt or otherwise protect such information. Your practice's Privacy Officer or other designated individual will assess all potential breaches to determine whether they are reportable. Your duty is to report any potential breach as soon as you discover it, so that it can be properly investigated, assessed and reported, if appropriate.

e-Compliance Training Test

HIPAA Privacy Rule - April 2019

NAME: _____ DATE: _____

SIGNATURE: _____ STAFF POSITION: _____

Return your test to your supervisor or Compliance Coordinator upon completion. Individual tests will be maintained to document participation and understanding of the information. Review the training information to find the correct answers to any questions that may have been missed.

1 Under the right of access, patients have the right to view or obtain a copy of all of their demographic, billing and clinical information that your practice has created, collected or maintains, with very few exceptions.

Select One **T** **F**

2 If a patient refuses to acknowledge that you've given him/her a copy of the Notice of Privacy Practices, you cannot proceed with treating that patient.

Select One **T** **F**

3 The Notice of Privacy Practices will describe the patient's privacy rights, and ways the practice may use and disclose PHI.

Select One **T** **F**

4 Prior to reporting a potential breach to your Privacy Officer, you should assess the potential breach to determine if it will be reportable.

Select One **T** **F**

5 You don't need a patient's authorization to disclose his/her PHI for marketing purposes.

Select One **T** **F**

6 As a workforce member, failure to comply with Privacy or Security Rule requirements could result in sanctions, loss of employment and/or personal legal liability for you, depending upon the nature of the incident.

Select One **T** **F**

7 The term protected health information (PHI) includes clinical information about a patient, but does not include billing or demographic information.

Select One **T** **F**

8 The Privacy Rule uses the term "individual" to refer to a patient or other person who is the subject of the information being collected/maintained/used/disclosed.

Select One **T** **F**

9 If a patient believes there is incorrect information in his/her record, he/she would request that an amendment be made.

Select One **T** **F**

10 The practice may require patients to request copies of their PHI in person for reasons of identity verification.

Select One **T** **F**

Table of Contents

Click Here to Take Your Quiz