

# e-Compliance Training

## Privacy Breach & Identity Verification - September 2020



THIS TRAINING SESSION IS RECOMMENDED FOR:

This training module is for all workforce members that view, use, or disclose protected health information (PHI). The term workforce member includes employees, volunteers, interns, residents, contracted and temporary workers and others.

### Training Objectives

The objectives of this training module are to ensure that participants:

1. Can define and identify potential privacy breaches/incidents;
2. Are able to follow reporting protocols;
3. Are familiar with sanctions and corrective actions for privacy incidents/breaches; and
4. Understand the identity verification process and its purpose.

### Defining Privacy Breaches

HIPAA's Privacy Rule defines a breach as an impermissible use or disclosure that compromises the security or privacy of PHI. The impermissible use or disclosure of PHI is presumed to be a breach unless your organization can demonstrate there is a low probability the PHI has been compromised based on a risk assessment.

If you realize that PHI has been disclosed to an unauthorized or improper person/entity, a potential breach has occurred, and you must report the incident to your Privacy Officer or other designated individual. That person will then document and assess the incident to determine whether it is reportable to the patient and the Department of Health and Human Services (HHS). At that time, sanctions, corrective actions, etc. will also be determined.

Common examples of potential breaches include mailing, faxing or giving PHI to the wrong patient, loss or theft of a portable device that was not encrypted, loss or theft of written materials that contain PHI, etc.

**Note** that information sent to the wrong provider will usually NOT constitute a breach, because it was disclosed to another covered entity, which is also bound to protect patient confidentiality. It will still be an internal violation that will be documented and will require corrective action, but notification to the patient and HHS will often not be required. However, it is important for you to simply report to your supervisor or Privacy Officer ALL incidents where PHI was sent or given to the wrong party, and your Privacy Officer will handle the process from that point forward, making a determination of whether the incident is a reportable breach.

If a breach of patient information occurs, the patient may desire to file a complaint either with your organization, or directly with the Office for Civil Rights (OCR). In addition, anyone can file a complaint on a patient's behalf. Although the OCR cannot investigate every breach report or complaint, it does investigate a certain number of reports that come in. During an investigation, you would be asked to upload various documents to a secure portal to demonstrate your compliance.



## 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.

Breaches can damage trust with your patients, and cost money in time and other resources for investigation, notification and remediation. If a breach affects more than 500 patients, local news media outlets must be notified. This can be harmful to your practice's reputation and can erode trust among patients. It is important for you to be diligent in reporting incidents for assessment, but to also do your part to prevent privacy incidents/breaches whenever possible.

### **Sanctions/Disciplinary Action**

If you cause/commit a privacy incident, you will be subject to sanction/disciplinary action. The sanction will depend upon the risk posed to PHI, the actual impact on a patient's privacy, malicious intent or lack thereof, and whether you've committed similar violations in the past. Sanctions can range from verbal warnings, written warnings, temporary suspensions and termination. Your organization may have sanctions that differ from these examples.

Sanctions must be applied fairly, meaning that if different staff members commit the same violation, they will receive the same sanction, unless there were aggravating or mitigating factors. In addition, management personnel and providers are also subject to sanctions.

### **Corrective Actions**

After a privacy incident occurs, there will often be corrective actions taken to limit recurrence. This is true even if it is determined that the incident is not a reportable

breach. Corrective action can include retraining, modifying processes, introducing new safeguards, etc.

Your Privacy Officer or management personnel will instruct you on any corrective actions that are necessary, and it is your responsibility to follow instructions for implementation. Actions taken to ensure privacy may seem inconvenient, as they may slow certain functions in order to verify identity, ensure information is going to the correct party, etc. However, such inconveniences are minor in comparison with the costs and effects of a privacy breach.

### **Common Safeguards**

#### *Paper Records*

If records are ever taken off site, there should be a system to record the date of checkout, the person removing the records/documents, and then to confirm that they get checked back in. If the records are ever lost or stolen during transit, you would then know which patient(s) to notify.

When transporting PHI, documents and media should be placed in a case, pouch or container to shield the contents from view. The container should be placed in the trunk if possible, to prevent it from inviting a break in, and the vehicle should always be locked if the PHI is left unattended in the vehicle.

There should be a secure process for shredding paper records that are no longer needed. If you have a shredding bin at your desk/workstation, it should be emptied



at the end of every shift into a bin/room/closet that can be locked until the documents can be securely shredded. This will prevent someone from inadvertently placing documents in the regular trash, which could result in a privacy breach. There may be a procedure for secure self-shredding, or an outside vendor may be used (which would be a business associate).

#### *Portable Media*

If you utilize any portable media that contains PHI, the device should be encrypted. Encryption of portable devices prevents a devastating breach in the event the device is lost or stolen. If you use a portable device, and save ANY document that contains ANY PHI, check with your Security Officer for instruction on the proper procedures for that device. Your Security Officer will implement encryption for portable devices and will set policy for saving documents to portable devices.

#### *Faxing/Mailing*

Workforce members should confirm fax numbers prior to hitting the send button when sending fax transmissions. If you have frequently used numbers stored in speed dial, those numbers should be checked periodically to ensure they are still correct.

When preparing a mailing, workforce members should verify that the contents of an envelope match the label. In addition, each page of documents should be checked to ensure that another patient's information doesn't get included in the wrong patient's envelope.

#### *Hand-Delivery of Documents*

When handing documents to patients, take an extra moment to briefly verify the patient's identity, and to confirm that all pages match before handing the documents over to the patient.

### **Identity Verification**

The Privacy Rule Standard 45 CFR 164.514 (h)(i) requires you to verify the identity of any person or entity that is not known to you prior to making a disclosure of PHI. Your organization will have identity verification procedures to follow. Note that you are not required to verify identity of persons already known—meaning that if your front desk staff know many of your patients, you don't have to go through full identity verification procedures every time they are seen. Identity verification may be required whether the request for disclosure of PHI comes from a person, a business entity, or another provider.

### **Sample Identity Verification Procedures**

The following examples outline methods that are commonly used to verify identity. Check with your Privacy Officer to verify specific procedures within your organization.

1. Requiring one piece of tangible identification (preferably a photo ID) such as a driver's license, military ID, employment identification badge or card, passport, or other government issued identification.
2. For persons requesting their own PHI, the name on the record should match their identification (or



they may have documents that verify a name change that has not yet been updated on their photo ID).

3. If the person requesting the PHI is not the patient, you should verify that there is a valid authorization in place that names the person as authorized to receive the information (or determine with your Privacy Officer that no authorization is required for a particular disclosure). This involves looking in the chart to locate an authorization signed by the patient. A valid authorization, signed by the patient, permits the practice to disclose the PHI indicated to the party named once identity verification has been completed.

### **Disclosures to Other Covered Entities**

There is a provision within the Privacy Rule that allows covered entities to disclose PHI for treatment purposes to other covered entities who are involved in a patient's care without patient authorization. Many entities either do not understand this provision or require an authorization as a precaution.

If you are already familiar with another practice who is requesting records for treatment purposes, you can make the disclosure. If you are unfamiliar, you can verify the practice by making an internet search, calling information to verify the phone number, etc. prior to making a disclosure. Many practices will make the disclosure without an authorization but require a simple written request from the other entity to aid in documenting the disclosure and to verify the destination to which information will be sent.

### **Subpoenas/Attorneys and Law Enforcement**

Specific requirements must be met to disclose information pursuant to a subpoena that is not court-ordered. For this reason, your Privacy Officer or other designated individual will review all subpoenas to ensure that requirements are met prior to making the disclosure. In addition, identity verification will be completed as part of the process.

Your Privacy Officer will handle requests from law enforcement, because there are specific requirements that outline when information may be disclosed, limits on what can be included in certain types of permitted disclosures, when a court order or warrant is required, etc. The Privacy Officer will also verify the identity of the law enforcement official prior to making a disclosure.

### **Documentation**

Whenever you perform identity verification procedures, you should document it in the patient's chart to demonstrate that you completed applicable identity verification procedures prior to making a disclosure. This will protect your practice from complaints about improper disclosures. ●



# e-Compliance Training Test

## Privacy Breach & Identity Verification - September 2020

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** If paper records/documents are taken off site, there should be a system to record the date of checkout, the person removing the records/documents, and to confirm that they get checked back in.

**Select One**      **T**      **F**

**2** Specific requirements must be met to disclose information pursuant to a subpoena that is not court-ordered.

**Select One**      **T**      **F**

**3** When handing documents to a patient in person, ask the patient to confirm that all pages are theirs before they walk away from you.

**Select One**      **T**      **F**

**4** If you have a bin of papers at your desk/workstation to be shredded, it should be emptied at the end of every shift into a bin/room/closet that can be locked until the documents can be securely shredded.

**Select One**      **T**      **F**

**5** The identity verification standard within the Privacy Rule requires that you check photo ID of patients at every visit to your practice/organization.

**Select One**      **T**      **F**

**6** If a breach of patient information occurs, the patient may desire to file a complaint either with your organization, or directly with the Office for Civil Rights (OCR).

**Select One**      **T**      **F**

**7** An impermissible use or disclosure of PHI is presumed to be a breach unless your organization can demonstrate there is a low probability the PHI has been compromised based on a risk assessment.

**Select One**      **T**      **F**

**8** If your actions resulted in an improper disclosure of PHI, you will institute corrective actions before notifying your supervisor or Privacy Officer.

**Select One**      **T**      **F**

**9** There is a provision within the Privacy Rule that allows covered entities to disclose PHI for treatment purposes to other covered entities who are involved in a patient's care without patient authorization.

**Select One**      **T**      **F**

**10** If a breach affects more than 100 patients, local news media outlets must be notified.

**Select One**      **T**      **F**