2022 Employee HIPAA Orientation (EHO) Handbook

Using EHO – The material in this booklet is designed to provide newly hired employees with an understanding of HIPAA's regulations and their impact on the employee and the practice.

Interactive Training – While the training materials are designed to be a self-study module, your Compliance Officer, supervisor, or manager can assist you with any questions. As with any new workplace orientation, it is critical that you clearly understand how your practice addresses compliance situations. Policies and procedures from your previous places of employment may differ from those of this employer. Your responsibilities for this training session are to review all of the material and ask questions to clarify any areas that are unclear.

Table of Contents

HIPAA Background

While the major focus of this training material will be on two of HIPAA's regulations, The Privacy and Security Rules, we will begin with a general review of the regulatory background.

Original Intent – The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress and enacted into law in August 1996. Its original purpose was to enable individuals covered by group health plans to take their healthcare coverage with them from one employer group to another group, which is reflected in the term "portability" within the HIPAA title.

As with any regulation, HIPAA has grown to be a lengthy and complicated piece of federal legislation. With the additions of standards to help fight fraud and abuse, protect the privacy of patients, ensure security of patient records, and an ambitious goal to eliminate paper transactions with electronic transactions, HIPAA is a challenge for every segment of the healthcare field. The Privacy Rule alone is almost 900 pages in length and makes other compliance documents seem simple by comparison.

HIPAA's Standards, Rules, and Acts

While insurance portability may have been the primary intent, HIPAA established multiple regulations that define the responsibilities for healthcare providers and business associates regarding patient information. Here is a brief overview of the regulations affecting HIPAA compliance:

1. **The Transactions Standard** - This standard applies to the electronic transmission of information outside of an organization or practice. This regulation has minimal direct impact on the patient.

2. **The Privacy Rule** - This Rule applies to protecting the privacy of personal information, known as protected health information (PHI), whether that information is stored electronically or in any other form. The Rule requires that healthcare practices implement written policies and procedures to ensure that all PHI is confidentially maintained. PHI includes any information that describes an individual's health status, demographic characteristics, or billing information, and that identifies an individual.

   All healthcare providers, health plans, healthcare clearinghouses, and business associates must comply with the Privacy Rule. The Privacy Rule gives individuals substantial control over who may access their PHI and the purposes for which that information may be used.

3. **The Security Rule** - This rule applies to any information collected, obtained, transmitted, or stored electronically by a covered entity (i.e., a health plan, healthcare provider, or healthcare clearinghouse) and any business associates of that entity. The Rule seeks to ensure the confidentiality, integrity, and availability of all electronic protected health information.

4. **National Federal Identifiers** - As Social Security Numbers are a unique identifier for individuals, every covered entity is assigned a National Provider Identifier (NPI) under HIPAA. All covered entities are now expected to be in compliance with this requirement.

5. **Enforcement Rule** - The Enforcement Rule provides guidelines relating to the investigation of HIPAA noncompliance. It also identifies the process for imposition of civil money penalties. Among other matters, the rule clarifies the investigation process, basis for liability, determination of the penalty amount, grounds for waiver, conduct of the hearing, and the appeal process.

6 **HITECH Act** – The Health Information Technology for Economic and Clinical Health (HITECH) Act included changes to the Privacy, Security, and Enforcement Rules. These changes were necessary due to the evolution of technology and administrative developments within the healthcare environment.

7 **Omnibus Rule** – Published January 25, 2013, the Omnibus Rule included changes to the Privacy and Security Rules, and HITECH Act.

HIPAA Definitions

Regulations tend to create new terms and a vocabulary that may be confusing. The following definitions will help you to understand the information for The Privacy Rule.

Protected Health Information (PHI) – PHI includes any information that identifies an individual and describes his or her health status, age, sex, ethnicity, or other demographic characteristics, whether or not that information is stored or transmitted electronically. It is similar to *Individually Identifiable Health Information* **-** information created or received by a healthcare provider, health plan, or healthcare clearinghouse that relates to an individual's physical or mental health, healthcare treatment, or payment for that treatment. Protected health information either specifically identifies the individual or could be used to identify the individual. PHI also includes any billing information that could be used to identify an individual.

Individual – In the Privacy Rule, the person who is the subject of PHI (i.e., a patient) is referred to as the individual. The individual or patient is bestowed many rights regarding his/her PHI under the Privacy Rule. While your practice may own the physical record of that information (i.e., the patient chart), the individual retains certain rights concerning how and when your practice may use that information (often conveyed to the patient in a Notice of Privacy Practices).

Healthcare Provider – This title applies to any individual or institution that furnishes, bills for, and is paid for healthcare services. Examples of individual providers are physicians, dentists, and other licensed healthcare practitioners. Examples of institutional providers include hospitals, nursing homes, home health agencies, rehabilitation services, clinics, and clinical laboratories. Suppliers of durable medical equipment are also considered providers under HIPAA.

Use and Disclosure of PHI – Disclosure and use are two different concepts under HIPAA. Understanding the difference will help you comprehend the Privacy Rule requirements.

Disclosure, under HIPAA, is defined as the release, transfer, provision of access to, or divulging, in any other manner, of information outside the entity holding the information. Examples of disclosure would include contacting a pharmacy with a prescription order for a patient, sending billing information to an insurance company, and any other sharing of the patient's PHI with entities outside of your practice.

Use, under HIPAA, is defined as the sharing, employment, application, utilization, examination, or analysis of individually identifiable information within an entity that maintains the information. Essentially, use occurs when a patient's PHI is acquired or viewed by workforce members, but has not been shared with any entity outside of your practice.

Treatment, Payment or Healthcare Operations - This defines how a patient's PHI may be used or disclosed by your practice for the purposes or processes of providing treatment to them, collecting payment for treatment, or other necessary uses and disclosures which affect the operation of your practice.

The Privacy Rule

The primary focus of The Privacy Rule is to protect individuals (patients) from unauthorized use or disclosure of their protected health information. PHI may be released or provided in two ways – intentionally and unintentionally.

Essentially, the Privacy Rule is a collection of responsibilities for healthcare providers and rights for patients pertaining to PHI. As you will see, the responsibilities and rights often overlap, but also have some differences for the provider or individual.

Rights of an Individual Under the Privacy Rule

Under HIPAA an individual is defined as the person who is the subject of PHI. Some of the rights of an individual under HIPAA include:

Right to Notice – Individuals have the right to receive a Notice of Privacy Practices from any healthcare provider from whom they receive healthcare services, any health plan in which they participate, and any healthcare clearinghouse that transmits or handles their PHI.

The Notice must include a list of the patient's rights (described below). Additionally, the Notice will include a description of how your practice will use and disclose PHI, and will explain that the practice does not need an authorization from the patient when using or disclosing information for the purposes of treatment, payment, and healthcare operations.

Your practice may include special notices that will allow your practice to use PHI to contact the patient regarding their healthcare, such as with appointment reminders, to provide information regarding alternative treatments, and about health-related benefits and services offered by your practice.

The Notice will also provide a listing of other reasons for disclosing PHI without patient authorization. These reasons are listed in the Privacy Rule and include:

- Disclosure of PHI to others involved in the patient's healthcare and identified by the patient
- To the FDA
- For legal proceedings
- As required by law
- For Public Health
- For communicable disease
- For health oversight
- In cases of abuse or neglect
- To law enforcement, and
- For research
- For military activity & national security
- For worker's compensation
- When an inmate
- To coroners, funeral directors
- To organ donation organizations
- When required by HHS to investigate and/or determine compliance by the practice.

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)). Review your practice's Notice so that you are familiar with its content.

Right to Authorize - A patient has the right to authorize any use or disclosure of PHI for a purpose not described in the Notice of Privacy Practices. If a patient refuses to authorize such uses or disclosures, they have the right to expect that their PHI will not be used or disclosed for such purposes. See your Compliance Officer for samples of the type of authorization forms that are used by the practice.

In simple terms, if your practice failed to identify, in the Notice of Privacy Practices, a purpose for which you will use or disclose PHI, then you may not use or disclose the information without special written authorization from the patient. Additionally, a patient has the right to deny signing an authorization, thereby prohibiting your ability to use or disclose the information for that purpose.

The most common example for required use of a patient authorization would involve disclosure to a family member, friend or other entity, identified by the patient.

Right to Designate a Personal Representative - A patient has the right to designate a personal representative who will be delegated with the authority to consent to or authorize the use or disclosure of PHI on the patient's behalf. A personal representative has the power to exercise all of the rights of the individual regarding the patient's PHI. However, this designation does not confer the right to make treatment decisions. In the case of a minor child, a parent, legal guardian or governmental agency with legal authority will act as the personal representative or may designate one for the child.

Right to Request a Restriction - A patient has the right to request that a practice not use or disclose certain PHI, and to request that the provider make reasonable efforts to keep the communications of PHI confidential. This type of request is known as a use and disclosure restriction.

A patient may request to restrict your practice from disclosing any part or all of his/her patient record to anyone outside of your practice for any reason. As a balance to this patient right, your practice

has the right to agree to or deny most requested restrictions. Your practice must provide a written notice of acceptance or denial for requested restrictions including an explanation for any denials.

One type of requested restriction that may not be denied is one restricting disclosure to a health plan concerning a treatment or service for which the patient (or someone on behalf of the patient) has paid out of pocket, in full. This is a requested restriction to which the practice must agree if the patient submits the request in writing, and the disclosure is not required by law.

Right to Disclosure Accountability – The Privacy Rule provides patients with a right to request and obtain an accounting (listing) of their PHI disclosures. The accounting must be provided to the patient within 60 days of the receipt of a request from the patient. The first accounting to a patient in any 12-month period must be provided at no charge.

The accounting should list all disclosures a practice has made, except that the accounting does not have to include disclosures that were made:

(1) To carry out treatment, payment, and healthcare operations;

(2) To patients about their PHI;

(3) Made as stipulated in an authorization signed by the patient;

(4) For a facility's directory or to persons involved in the patient's care;

(5) For national security or intelligence purposes;

(6) To correctional institutions;

(7) As part of a limited data set; or

(8) Prior to the compliance date of the Privacy Rule.

Right to Access - A patient has the right to access, inspect, and obtain copies of PHI maintained by a healthcare provider, health plan, or healthcare clearinghouse. This means that the patient has the right, with few exceptions, to access all PHI that a practice has collected, created, and maintained on him/her. This means the patient may request:

- To inspect his/her patient record maintained by your practice. He/she also has the right to review all of the notes made by your practice and information that you have collected from other providers (with the exception of psychotherapy notes and information that was intended for use in a civil, criminal, or administrative action). A patient must submit a written request to the practice to review his/her record, and will be supervised by a workforce member during the inspection of records.

- A copy of his/her patient record. HIPAA rules limit the fees that may be charged to a patient for copies of his/her medical records. Your practice may charge a reasonable, cost-based fee.

- A patient also has the right to request that copies of his/her records be forwarded to a third party, such as a life or car insurance company, attorney, etc. HIPAA rules do not limit the fee that may be charged in these cases, however, State guidelines should be followed, if applicable.

Right to Request an Amendment – Patients may request amendments to their PHI. This means they may ask you to add a note or amendment to an item in their medical record if they feel there is erroneous information therein. While the original record cannot be changed, an amendment can be added to a record noting the individual's request. If your practice agrees to the requested amendment, it must become part of the individual's record.

The practice has the right to agree to or deny such requests. If your practice agrees to a requested amendment, you must:

1. Make the required amendment to the PHI or records that contain the information to be amended;

2. Inform the patient that the requested amendment was accepted (preferably in writing);

3. Ask the patient to identify persons or entities that should be notified of the amendment and obtain the patient's permission to contact those persons or entities; and

4. Make a reasonable effort to inform the following two groups about the amendments:
    - persons identified by the patient; and
    - persons, including business associates, to whom you have disclosed the information who could be predicted to use the information to the detriment of the patient. Notification of the amendment does not have to be sent to all persons or entities that received the information to be amended. Your practice is only required to notify persons or entities that may have used, or are likely to use the information in the future to make decisions that could be detrimental to the patient.

A 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.

The practice will act on a request for amendment within 60 days. A 30-day extension may be permitted under certain circumstances, but it is expected that the efficiencies of retrieving, verifying and updating information in electronic format should enable compliance with the 60-day timeframe, or perhaps an even shorter timeframe. In addition, the Privacy Rule allows the covered entity and the individual to agree to conduct any written exchanges electronically in order to expedite the process.

Responsibilities of a Practice or Other Provider Under the Privacy Rule - Having reviewed the rights of the patient, we will now look at the responsibilities of the provider (your practice). You will notice that they mirror most of the patient's rights.

- **Notice of Privacy Practices** – A practice must provide the patient with a copy of its Notice of Privacy Practices that describes the intended uses and disclosures of PHI. Additionally, the Notice must be posted in the patient waiting area, and posted on the practice's website, if applicable.

- **Acknowledgement of Receipt** – A practice must attempt to obtain patients' acknowledgement of receipt of the Notice of Privacy Practices. This is a simple statement signed by the patient that documents that they were provided with a copy of the Notice. Obtaining an acknowledgement of receipt need only be performed once, even if the Notice is later revised.

- **Patient Authorization** – The practice must obtain specific written authorization for any disclosure or use of PHI other than for the purposes of treatment, payment, or healthcare operations (see definitions). This refers to the patient's right to authorize uses or disclosures not addressed in the Notice of Privacy Practices.

- **Restrictions** – The practice must make reasonable efforts to preserve the confidentiality of certain communications of PHI when requested to do so by an individual. This refers to the individual's right to disclosure restriction. As previously stated, the practice can agree to or refuse a requested restriction with the exception of a disclosure to a health plan when the patient has made payment out-of-pocket in full and requested such a restriction in written form.

- **Access to PHI** – The practice must provide access to PHI that it has collected, created and maintains regarding the individual. As previously stated, the patient has the right to access almost everything you maintain in his/her record, including demographic, clinical and billing information.

- **Amendments** – The practice must make reasonable efforts to correct possible errors in protected health information when requested to do so by an individual. This refers to the individual's right to request amendments to his/her medical record. The practice may agree to or deny such requests.

- **Complaints** – The practice must establish procedures to receive complaints relating to the handling of PHI. Under the Privacy Rule your practice must have a process for receiving patient complaints about your privacy policies and procedures. The Supplemental HIPAA Training Information page at the end of this document (page 16) will indicate who in the practice will receive and respond to patient complaints.

- **Business Associate Agreements** – The practice must establish agreements or contracts with business associates to whom the practice discloses PHI for specified business purposes. Business associates are required to handle PHI in the same manner as the provider. A business associate is a person or entity that your practice will intentionally give PHI, or provide access to it for the purpose of that entity performing a service for the practice. Examples of business associates include EHR and telehealth vendors, outside transcription services, billing companies and collection agencies.

- **Patient Authorizations and Other Disclosures -** Disclosure of PHI and authorizations are perhaps the most important requirements of The Privacy Rule. This is why we will address these areas specifically, in addition to overviewing them as part of an individual's rights and a provider's responsibilities (see below).

- **Treatment, Payment, Healthcare Operations** – The concept of treatment, payment, and healthcare operations is intended to prevent HIPAA rules from impeding the delivery of healthcare.

  The Privacy Rule generally prohibits a practice from using or disclosing PHI unless authorized by patients, except where this prohibition would result in unnecessary interference with access to quality healthcare, or with certain other important public benefits or national priorities. Ready access to treatment and efficient payment for health care, both of which require use and disclosure of PHI, are essential to the effective operation of the healthcare system. In addition, certain health care operations—such as administrative, financial, legal, and quality improvement activities—conducted by, or for, healthcare providers and health plans, are essential to support treatment and payment. Patients expect that their health information will be used and disclosed as necessary to treat them, bill for treatment, and, to some extent, operate the covered entity's healthcare business.

  To avoid interfering with a patient's access to quality healthcare or the efficient payment for such healthcare, the Privacy Rule permits a practice to use and disclose PHI without a patient's authorization if it is for the purposes of treating the patient, obtaining payment for services, or as part of certain business operations for the practice. For other purposes, authorization is required.

- **Authorizations** - Essentially, there are two types of authorizations that you need to understand under The Privacy Rule. First is the authorization for a Personal Representative and the second is a more limited form of authorization.

  Personal Representative - As previously stated, the patient has the right to designate a Personal Representative. The personal representative has the power to exercise all of the rights of the patient with regard to use or disclosure of the patient's PHI. A Personal Representative can designate additional Personal Representatives, make other authorizations, request restrictions and amendments, access PHI of the patient, and obtain copies of the PHI. This designation on its own does not confer the right to make treatment decisions on behalf of the patient.

  An authorization for a Personal Representative is normally valid until revoked by the patient, the Personal Representative, or another entity that has legal authority to do so.

  - **Other or Limited Authorizations** – A patient may also make a more limited type of authorization in which they authorize or give the practice permission to disclose a part or all of the patient's PHI to another person or business entity. An example would be if a patient wishes a family member or friend to receive a specific lab test result, medical history, or surgical information. In another example, a patient may authorize the practice to disclose his/her entire medical record to an attorney or other entity.

A limited authorization will identify to whom the practice may disclose information, what information is to be disclosed, and will include an expiration date and signature of the patient.

It is important to become familiar with the authorization forms utilized by your practice. Ask your supervisor or Compliance Officer for clarification should you have questions regarding use of authorization forms.

Conversations, Faxes, and Phone Messages – Conversations involving PHI may be overheard in medical and dental practices, pharmacies, hospitals, laboratories, and all other healthcare facilities. Overheard conversations are identified in the Privacy Rule as "incidental disclosures" and are not a violation of HIPAA rules, provided that reasonable safeguards have been followed.

A practice must implement reasonable safeguards that ensure the confidentiality of PHI when making phone calls to patients, faxing or emailing PHI, and discussing PHI with patients or other staff members of the practice. Examples of reasonable safeguards would include:

- **Confidential Conversations** – Staff members should be aware of their environment when making phone calls and having discussions with other staff members or patients regarding PHI. A reasonable safeguard is to speak in a lower than normal volume to limit others from overhearing conversation involving PHI.

- **Phone Calls** – Staff members should ensure that limited information is left when the patient is not available to receive a phone call from the practice. Messages left on voice mail, answering machines, or with individuals other than the patient should be limited to the name of the practice and a phone number for the patient to call back. Appointment reminders may be left, as mentioned in the practice's Notice of Privacy Practices, but should be limited to the day and time of the appointment with a phone number to call if the patient should need additional information. Check with your Compliance Officer to identify your practice's procedure for leaving phone messages.

- **Facsimile/Email Messages** – PHI may be faxed or emailed if reasonable safeguards are followed:
  - When faxing information to other providers, hospitals, laboratories, and other entities involved in the treatment of the patient, verify the fax number of the intended recipient.
  - Emailing or transmitting EPHI via electronic fax (i.e., through Internet connection) requires encryption of the data to prevent a privacy breach, should the transmission be intercepted.
  - If a patient requests that the practice email or electronically fax his/her EPHI, he/she must be informed of the risk of interception if encryption is unavailable, and if the patient accepts the risk, the request should be honored and documented in the patient's chart.
  - When faxing or emailing information upon patient request, verify the fax number or email address and document the request in the patient's chart. Verify the patient's name and date of birth to ensure the correct information is sent.

Confidentiality Requirements - The Privacy Rule requires a practice to maintain the confidentiality of a patient's PHI. The Rule also holds a practice responsible for ensuring that its employees, agents, and vendors or business associates are accountable for the confidentiality of PHI.

Your employer may require you to sign a confidentiality agreement. This is a standard business requirement and enables your practice to document that it has communicated its expectations to you regarding confidentiality. Note that your responsibility for maintaining the confidentiality of PHI extends beyond your term of employment/association with the practice.

The Rule also has a requirement known as "minimum necessary information". This applies to PHI that you access within the practice as well as PHI that you disclose to entities outside of the practice. This rule requires that you only access PHI that is required for the performance of your assigned duties. The goal is to ensure that the PHI of a patient is only used as necessary for treatment, payment, or healthcare operations.

Minimum necessary information also applies to PHI that is disclosed to entities outside the practice. An authorization or request for PHI will identify how much PHI is to be disclosed. In some cases, it may be necessary and appropriate to disclose the patient's entire medical record. However, if this is not the case, you must ensure that only the minimum necessary information is disclosed. Please note that the minimum necessary standard does not apply to disclosures made for treatment purposes.

Identity Verification Policies

HIPAA's Privacy Rule recommends the use of identity verification in order to limit the potential for disclosure of PHI to unauthorized individuals. Specifically, the Privacy Rule requires a practice to verify the identity of a person or entity with whom the practice is unfamiliar when fulfilling requests for disclosure of PHI. The use of identity verification is an excellent method for preventing privacy breach incidents.

Identity theft can range from fraudulent use of credit cards to a complete takeover of another person's identity. Perhaps one of the more common uses of another person's identity occurs when a person obtains services under another person's insurance. For a practice, the cost of a fraudulent insurance claim will come back to the practice the same as a fraudulent credit card charge.

With the responsibility of protecting patient information, the use of identity verification is a control measure that helps to limit disclosing of information in an unauthorized manner.

HIPAA's Privacy Rule includes a verification standard (45 CFR 164.514(h)(i)) that provides a practice with the right to require oral or written documentation, statement, or representation of the identity and authority of any person to have access to patient information if the identity or authority is unknown. Simply put, the Privacy Rule allows practices to require verification, if the practice is not sure of the identity of the person or entity making the request.

Identity verification can be required (assuming your practice is unfamiliar with the identity of the person or entity requesting the information) whether the request for disclosure of PHI comes from an individual (the patient or another person), a business entity, or another provider (another practice, a hospital, etc.) as part of compliance with the Privacy Rule.

Examples of Identity Verification Procedures

The following examples of identity verification procedures are intended to serve as a guide for common occurrences in healthcare. Check with your practice's Privacy Officer to confirm the recommended procedures for your practice.

A Request for PHI Made in Person - This is a request that will normally be made by a patient or his/her authorized representative. If the patient is known to the practice (i.e., the employee handling the request knows the patient by sight verification or possible photo match from your EHR system), you could process the request without further verification procedures. If the patient or person is unknown to the practice, identity can be verified by:

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. If the person is requesting his/her own patient information, the name on the record should match the identification.

3. If the person requesting the PHI is not the patient listed on the record, you should verify that he/she is an authorized representative. This means looking in the chart for an authorization signed by the patient. An authorization, signed by the patient, gives another person the authority to access all or part of the patient's information, depending upon the *type* of authorization.

If there is a discrepancy with identification, or for cases in which you are unable to satisfactorily verify the identity of the person making the request for PHI, you may refer to the individual in your practice that is designated to handle these situations. The individual is identified on the Supplemental HIPAA Training Information page at the end of this document (page 16).

Requests by Another Practice or Other Covered Entity – Requests for patient information may also come from other practices or covered entities. Such requests may be made by telephone or mail.

When requests for patient information are made by telephone, you may use various methods to verify the identity of the caller if unknown to your practice. You may inform the caller that you will return his/her call and use a published phone number (obtained through Internet search or other method) to make the return call. If there are no discrepancies, and the caller can be reached through the entity's published number, you may fulfill the request for disclosure. Verification of mail requests can be handled in a similar manner. Verify that the mailing address provided in the request matches the covered entity's published address.

Privacy Breach Notification

Growing concern over the security of personal information has resulted in a HIPAA requirement for providing patients with notification in the event of a breach or unauthorized disclosure of PHI. It is believed that notification will enable a patient to mitigate financial or other harm that could result from the breach.

A breach is defined as an unauthorized acquisition, access, use or disclosure of unsecured PHI (that compromises the security or privacy of such information) by a member of the practice's workforce, person working under the authority of the practice, or a business associate of the practice. A privacy breach may involve printed or electronic formats of PHI.

A breach of PHI could include a lost or stolen device (i.e., computer, smart phone, etc.) that has unsecured patient information stored on it. An unsecured flash drive or other mobile media, such as a CD or DVD containing patient information, would also present a possible breach. A lost chart or other printed material containing patient information would also be considered a potential breach, because you cannot encrypt or otherwise protect such information. Faxing a patient's information to the wrong fax number also constitutes a potential breach of unsecured PHI (if it is faxed to an unknown entity or to a recipient that is not also subject to HIPAA regulations).

PHI is considered secure if it has been rendered unusable, unreadable, or indecipherable to unauthorized individuals (using technologies and methods specified by HHS). This means that the information has been encrypted or, in the case of printed hard copy materials such as medical records, shredded or otherwise destroyed so that it can neither be read nor reassembled.

Discovery of a Breach - Every member of the workforce should be alert and notify the Privacy Manager if there is a reason to believe that a privacy breach has occurred. Upon discovery of a breach, a practice is required to begin and document a complete investigation of the incident. An investigation enables a practice to determine whether a breach has occurred, identify the source or cause, take corrective actions to limit any recurrence, and gather information it needs to provide to patients affected by the breach.

Notification to Patients, Media and HHS - Following a breach, a practice is required to make notification to the patient(s) as soon as is reasonable, but no later than 60 calendar days after the discovery of a breach by the practice. The intent is to make a notification as soon as there is confirmation of the breach. If needed, a practice may provide all of the required information to the patient in multiple notices, as the practice obtains the information.

A practice is required to provide notification to media (print or broadcast) for a breach that involves 500 or more residents of a State or jurisdiction. Notices to the media are in addition to those provided for individuals and are not meant to replace the notice to individuals. Additionally, the practice is required to notify the Department of Health and Human Services (HHS) of all confirmed breaches. Breaches involving 500 or more individuals will require immediate notification to HHS, while smaller breaches will be reported after the end of the calendar year in which they occur.

THE SECURITY RULE

The Security Rule is focused on the security of PHI that is collected, created, or maintained by the practice in an electronic format. The Rule has created a new term, electronic PHI or EPHI to identify PHI in this format.

The majority of compliance tasks stemming from the Security Rule are accomplished at management and operational levels. However, there are parts of the Rule that affect the duties of employees who have access to EPHI. The following information addresses security issues of which you should be aware.

Protection from Malicious Software – Examples of malicious software, or malware, include viruses, Trojan horses, worms, spyware, and ransomware. There are many types of malware that can infiltrate information systems with the intent of corrupting, damaging or stealing information. There are things that you can do to prevent a malware attack:

- Malware is often acquired through malicious email attachments, or email links that appear to come from friends, reputable companies and organizations, or other trusted sources. This fraudulent practice is known as phishing and remains one of the most effective tactics for stealing user credentials and other sensitive information. Caution should be exercised before opening email attachments or clicking links embedded in an email message. Many email programs have the ability to scan messages and their attachments and prevent you from opening those that are likely to cause harm. Use any such feature that is available to you.

- There are many websites that are infected with various malware, and more sophisticated malware has been known to automatically download even when a mouse is only moved over a link (without clicking it). Avoid visiting unknown websites, and do not use the practice's information systems or equipment for personal reasons.

- Outside media (i.e., CDs, DVDs) and software (through download or portable media) are also common sources of malware attacks. The Security Officer must approve use of any outside media or software download and may require scanning the media or other measures to protect information systems. Even mobile phones can be infected with malware. Do not connect a mobile phone to your computer or the network without approval from your Security Officer.

- If you have been asked to run malware or virus scans on your workstation, be certain that you comply, and do so at the intervals requested (e.g., daily, weekly, etc.).

- If you are requested to update software or firmware (that often include security patches for vulnerabilities that have been identified), do so in a timely manner.

- If you realize that a link that was clicked on, a file attachment opened, or a website visited may have been malicious in nature, take immediate steps to limit the potential damage to your workstation or the network. Your Security Officer will communicate the specific steps to follow after

a known or suspected ransomware or other malware attack, such as shutting down your workstation and disconnecting it from the network. See the Supplemental HIPAA Training Information on page 16.

- After these initial steps are complete, immediately report any unusual messages, errors or functions that you suspect are indications of malware to your supervisor and/or the Security Officer.

Log-in Monitoring – Some information systems have the capability to monitor login attempts and will lock out a user after a certain number of unsuccessful attempts. If you receive a notice or message that unsuccessful attempts to access the system (under your user ID) have been made, or that your user ID has been locked out, notify a supervisor or the Security Officer to investigate a potential problem. Being observant of unusual messages or warnings may lead to the discovery of unauthorized access, tampering, malware, etc.

Password Management – Sharing of individually assigned computer access codes and passwords is considered a security incident and would result in sanctions for those persons involved. Essentially, the security of your password is your responsibility. Do not post your password in a location it could easily be discovered. If you must write it down, hide the password in a discreet location. You are not only required to keep your login credentials confidential, but you must also comply with any requests to periodically change your password and to adhere to password complexity requirements. If someone requests that you share your user ID and password, notify your supervisor or the Security Officer.

Mobile Devices – Mobile devices, such as tablets, smart phones, laptops, etc. that store EPHI require security measures. The Security Rule allows for flexibility in the methods used for securing such devices, because there are not standard software/hardware capabilities across all devices. The use of measures such as encryption, remote disabling/remote wipe, passwords and security software are all possibilities. Check with your Security Officer or supervisor if you have questions regarding the use of mobile devices.

Security Incidents – A practice is required to ensure its employees and agents comply with the requirements of the Privacy and Security Rules. Security compliance is accomplished by awareness, training, and the imposition of sanctions. Additionally, the practice is required to identify what would be considered security incidents or violations to the practice's security policies and procedures. Security incidents would include, but not be limited to:

- Failure to safeguard passwords and other system access - including sharing of a password with another staff member, or unauthorized individual or entity outside of the practice, using the password of another authorized user, or failure to report knowledge of any misuse of access IDs or passwords to the Security Officer or an immediate supervisor.
- Attempting to or successfully accessing, using or disclosing PHI in an unauthorized manner - including accessing PHI that is not required for the performance of one's assigned duties.
- Unauthorized disclosures of PHI, whether intentionally or through neglect.
- Unauthorized modification, interference or destruction of information systems or PHI.

- Use of unauthorized media in the practice's information system (even if no harm is caused).
- Connecting a cell phone or other unauthorized device to computer equipment that is the property of the practice.
- Failing to report suspected security incidents to the proper persons in the practice.

Sanctions

Sanctions are required to be imposed upon any workforce member who fails to comply with the practice's policies and procedures. The Privacy and Security Rules require the imposition of sanctions in order to encourage compliance by every workforce member.

Imposed sanctions will vary depending on the severity of the violation, the intent of the workforce member, and/or the fact that multiple violations (past and present) have been committed. Depending on these factors, sanctions may range from verbal reprimands and retraining, to termination of employment.

HIPAA Summary

HIPAA's regulations involve thousands of pages of requirements and an ever-changing list of interpretations. The information in this initial training program is designed to provide you with a general overview and a focus on a few specific issues related to privacy and security. You will also be required to participate in annual training, as required by HIPAA regulations.

The details of how your practice achieves compliance are in the specific procedures, forms, and information utilized by your practice. As a new employee, it is critical that you ask your supervisor or Compliance Officer for clarification when in doubt as to a correct action. It is better to ask questions, ensuring you are doing the right thing, than to make an assumption that may trigger patient complaints and possible inquiries from regulators.

Supplemental HIPAA Training Information

1. Name of the designated Privacy Manager:

   _____

2. Name of the designated Security Officer:

   _____

3. Identify the immediate steps a workforce member should take in the event of a ransomware or other malware attack:

   _____

   _____

   _____

3. Identify the individual(s) who are designated to handle the following situations:

   - patient complaints_____
   - security incidents_____
   - potential privacy breaches_____
   - PHI requests (including from attorneys)_____
   - identity discrepancies_____
   - patient authorizations_____

4. Provide a copy of the Notice of Privacy Practices that is currently in use.

2022 Employee HIPAA Orientation Training Test

Name:_____ Date:_____

Please enter your **true** or **false** answers below. You may discuss any questions with your Privacy Manager or Security Officer.

On-Line Testing – If you will be using Eagle Associates' web-based training program, you should complete the test in paper form prior to logging in to the online system.

1. [ ] Your password may be shared with another person as long as he/she is an employee of the practice.
2. [ ] Malware is often acquired through malicious email attachments, or email links that appear to come from trusted sources.
3. [ ] As a workforce member of the practice, you may be asked to sign a confidentiality agreement, which will outline your responsibilities with regard to safeguarding PHI.
4. [ ] A patient has the right to access, inspect and obtain copies of his/her protected health information (PHI).
5. [ ] Protected health information includes only a patient's health status and clinical information.
6. [ ] The Privacy and Security Rules require the development and use of sanction policies to encourage compliance with established policies and procedures.
7. [ ] The Security Rule applies to any protected health information collected, obtained, transmitted, or stored electronically by a covered entity.
8. [ ] The practice does not have the right to deny a patient's request to amend his/her PHI.
9. [ ] You may bring in outside media from home and connect it to your workstation/network as long as you believe it is free of viruses.
10. [ ] A breach is defined as an unauthorized acquisition, access, use or disclosure of unsecured PHI (that compromises the security or privacy of such information) by a member of the practice's workforce, person working under the authority of the practice, or a business associate of the practice.

Click Here to Take Your Quiz