e-Compliance Training

HIPAA Security Rule - May 2021

THIS TRAINING SESSION IS RECOMMENDED FOR:

This annual training topic must be completed by all members of a healthcare organization's workforce. This includes employees, contracted staff, volunteers, interns, residents, and students with access to its information system, etc.

Training Objectives

The objectives of this training module are to:

- explain workforce member responsibilities within the Security Rule;
- provide annual retraining on protection from malicious software, login monitoring and password management topics;
- outline the need to report security incidents; and
- identify sanctions for failures to follow security policy and procedure.

The Security Rule applies to all media, hardware, devices, equipment, etc. that store electronic protected health information (EPHI). This includes anything that is connected to your network that could be an access point for malware/bad actors. There are a variety of administrative, technical, and physical security safeguards for covered entities to implement that will ensure the confidentiality, integrity, and availability of EPHI.

The Security Rule is flexible and scalable, and the measures selected are dependent on the size and complexity of your organization, infrastructure, costs, and likelihood and possible impact of the risks to EPHI. This means that there are a variety of methods, software, mechanisms and procedures that can be deployed to comply with Security Rule standards. The Rule does not require use of any particular software or method to meet the requirements. For example, your organization may choose from a vast number of encrypted email vendors to protect data during transmission. Alternatively, secure file sharing services or secure patient portals are also often used to protect EPHI during transmission.

Administrative Safeguards

Security Management Process - Your organization must identify and analyze potential risks to EPHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level. Your Security Officer will complete what is known as a Security Risk Analysis.

Security Personnel - Your organization will have designated someone to serve as the security official who is responsible for developing and implementing its security policies and procedures. Ask your supervisor who has the role of Security Officer for your organization.

Information Access Management - The Security Rule requires a covered entity to implement policies and procedures for authorizing access to EPHI only when such access is appropriate based on the user or recipient's role. Because of this requirement, you will likely have a privilege set in EMR/EHR and practice management systems. That privilege set allows you to perform/access only the functions needed to accomplish your work duties. Some settings are so small that global access privileges are needed for users who

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.

are cross-trained. Even then, admin-level privileges are not granted to regular users.

Workforce Training and Management - Your organization must provide for appropriate authorization and supervision of workforce members who work with EPHI. All workforce members must receive training regarding security policies and procedures, and must be aware that sanctions will be imposed against workforce members who violate its policies and procedures.

Evaluation - A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule and how they continue to protect EPHI.

Physical Safeguards

Facility Access and Control - Your organization will limit physical access to its facilities while ensuring that authorized access is allowed. Your facility might have an alarm system, or security cameras, regular locks and keys, key cards, key codes or fobs, etc. Only persons who need means of access (such as a key, fob, card, etc.) will be granted it, and if you've been given a key, that fact will be recorded.

You will also likely be expected to help control access of patients and visitors to treatment and business areas of the practice. For example, patients and visitors should be escorted from waiting areas to exam rooms and other destinations in the practice to prevent tampering or theft of EPHI and related equipment.

Workstation and Device Security - Your organization will implement policies and procedures to specify proper use of and access to workstations and electronic media. There will also be policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of EPHI. You are responsible to ensure you don't allow unauthorized access to your own workstation. For example, you should log off if you know you are walking away from your station. The other items in this specification are likely handled by your Security Officer.

Technical Safeguards

Access Control - There will be technical policies and procedures that allow only authorized persons to access EPHI. Your login credentials grant access into your workstation, the network, the EMR/EHR and practice management systems, as appropriate. As previously mentioned, your login is set up in a way that grants you access/ability to do only the things needed to perform your work duties.

Audit Controls - Hardware, software, and/or procedural mechanisms will record and examine access and other activity in information systems that contain or use EPHI. Your Security Officer has the ability to track your activity within systems, and use it to investigate suspected improper access, errors, etc.

Integrity Controls - Policies and procedures will be in place to ensure that EPHI is not improperly altered or destroyed. Electronic measures will also be deployed to ensure that EPHI has not been improperly modified or destroyed.

Your IT person/department/vendor, in coordination with your Security Officer, will have implemented several different mechanisms to help ensure integrity of data.

Transmission Security - Technical security measures guard against unauthorized access to EPHI that is being transmitted over an electronic network. You might have a patient portal for secure communications, or encrypted email system/software. Secure file sharing services are also often utilized. Another method of ensuring security during transmission is using a secure software program or Virtual Private Network (VPN) for anyone who needs to remotely access data on your network.

Security Incidents

Common examples of security incidents include, but are not limited to:

- sharing a password;
- failure to report known security incidents;
- bringing in outside media and connecting it to the network without having it scanned or approved;
- attempted or successful unauthorized access/disclosure of EPHI; and
- failure to follow proper protocols for securely transmitting EPHI.

If you fail to comply with your organization's security policies and procedures, you will be subject to disciplinary action, also known as a sanction or penalty. Sanctions/penalties may include a verbal warning, written warning, suspension, or termination of employment (depending upon the circumstances). Your organization's sanction policy may vary from these examples. Sanctions will be applied equally to workforce members, regardless of rank or position, unless there were aggravating or mitigating circumstances surrounding the incident.

You will receive security reminders, initial and annual training on security, and instruction on policies and procedures to help you avoid security policy violations.

Minimum Necessary Standard

"Minimum necessary" is a concept that applies under both the Privacy and Security Rules, and requires that you access, use and disclose only the patient information that is needed to perform your duties or functions. In the course of your work, you will generally view, make use of, and disclose the minimum amount of information needed to perform a given task. There are exceptions to the minimum necessary standard, such as when PHI is disclosed to another provider for treatment purposes.

It is important to note that the minimum necessary standard applies to the ***access*** of patient information, as well as use and disclosure. This means you may not browse the information of any individual, including yourself, friends, family, celebrities, etc., unless you are required to access that information as part of your job duties. If you are a patient of the practice you work for and would like a copy of your own medical record, you should request it through the same process that any other patient would. You would be subject to disciplinary action for any access, use or disclosure of patient information that is not in compliance with the minimum necessary standard. Check

with your HIPAA compliance officer if you have questions about the minimum necessary standard or exceptions.

Acceptable Use

Your organization will have rules for proper use of your workstation, including sites you may visit on the Internet. You may be asked to read and sign an "Acceptable Use" policy upon hire, or to follow rules in an employee handbook. In addition, your network may have security settings in place that only permit access to web sites that are necessary to perform your functions.

Social Media

Your organization may outline permissible use (if any) of social media. Even if your organization has a presence on a social media platform, and even if a patient reaches out via social media, you should never publish any EPHI on a social media site/platform. You would always reply via a private method (phone, encrypted email, patient portal, etc.) in response to a social media inquiry, if EPHI would be needed in the reply. Recent breaches and potential data mining from social media are cause for increased vigilance.

Required Training Topics

There are three required areas of awareness/training within HIPAA's Security: protection from malicious software, login monitoring and password management. You play a role in helping to ensure the security of EPHI, and your understanding of these topics is your responsibility.

Protection from Malicious Software - Malicious software/malware can be a computer virus, disruptive code, ransomware (which locks files and asks for a payment to obtain a decryption code), spyware (which can capture keystrokes to obtain passwords and more), etc. Malicious software is often spread through email attachments or links, and in links on web sites. You should exercise caution whenever you receive an email with an attachment. Even if the sender is known to you, remain cautious, because a person's email can get hacked, and the hacker then sends out malware through the victim's email account. If you receive an email from someone you know, but the message seems unusual, and/or there is an unexpected attachment, contact the sender or your Security Officer before opening the attachment.

Some web sites, even those that seem harmless, can download malware in the background when you click links. For this reason, you must exercise caution in visiting web sites. In addition, your organization may have installed web filtering software that prevents you from visiting certain sites. There may also be a policy that requires you to limit web site usage to sites that are required for your duties.

You should neither bring in outside media nor connect it to your computer/network without approval from your Security Officer. Outside media includes CDs, DVDs, flash drives, removable hard drives and even cell phones. Cell phones can be infected with malware, which could migrate to the system when the cell phone is connected to a computer. If you need to charge your phone at work,

bring a wall plug and charge it directly. Some organizations do not allow any outside media, while others allow it only after it has been scanned/checked by an IT professional and cleared for use.

Ransomware – Ransomware is a specific type of malware that locks up or encrypts files on a computer, network, or server, and then asks the victim to pay money to unencrypt the files and regain the ability to access the data. All staff members should be aware of the potential indicators of ransomware, because early detection can prevent some of the damaging effects. In addition to being aware of indicators, immediate reporting is key to halting the spread and harm of malware. If you notice any indication of ransomware or other malware, report it as soon as possible to your Security Officer so that an appropriate investigation can be made, and steps taken to limit harm. A list of potential indicators of ransomware follows:

- a user's realization that a link that was clicked on, a file attachment opened, or a website visited may have been malicious in nature;
- an increase in activity in the central processing unit (CPU) of a computer and disk activity for no apparent reason (due to the ransomware searching for, encrypting and removing data files);
- an inability to access certain files as the ransomware encrypts, deletes and re-names and/or relocates data; and
- detection of suspicious network communications between the ransomware and the attackers' command and control server(s) (this would most likely be detected by IT personnel via an intrusion detection or similar solution).

Your Security Officer will communicate to you a list of specific steps to follow after a known or suspected ransomware or other malware attack. This may include shutting down your workstation, and disconnecting it from the network, etc. Be sure to have these steps handy now to ensure you are able to take quick action in the event of a malware incident. Some steps that may seem desirable, such as preemptive credential resets, may alert the intruder that you are aware of their presence. Always follow the instruction of your Security Officer for specific malware response steps to limit malware spread.

Phishing Schemes – In a phishing scheme, an attacker impersonates a trusted source, sends an email that appears to be from that source, and then tricks the user into divulging sensitive information or clicking links that contain malware. The logos and images in these emails often appear identical to those of the real company/entity. When clicking the links in phishing emails, users are taken to web sites that look like the site of the trusted source, but the URL may differ very slightly (using numeral 1s in place of letter ls for example).

It is important to use extra caution when opening email messages. If, after opening, you suspect it may be a phishing attack, do not click any links. Check the sender's email address by hovering over it to view the sender's

domain. If the domain doesn't match that of the trusted source, delete the message without clicking any links or images. If you suspect you've become a victim of a phishing attack, shut down your station immediately, disconnect it from the network, and contact your Security Officer for next steps or follow procedures that have been communicated in advance.

Login Monitoring – Monitoring your login process presents an opportunity to alert your organization to a potential security issue within the information system. When you start up a station and access the network and/or the EHR/EMR/PM systems, you are required to log in. Your login credentials verify your identity and access privileges. The use of an invalid log in will result in a denial of access, and the system may only allow a limited number of attempts before the computer locks down to prevent further operation. The locked-out user would have to see his/her supervisor, or the Security Officer/IT department to regain access. Such control measures help ensure that only authorized individuals are accessing EPHI, and prevent an unauthorized person from guessing at a password.

When logging in, you should observe and be aware of any unusual behavior, errors, messages or alerts that occur. If you receive an alert, warning or error message, immediately notify a supervisor and/or your IT personnel or Security Officer, so that they can investigate the situation. Failure to recognize and report unusual login events may lead to significant risks to EPHI.

Password Management – Passwords are codes that you use to gain access to information or information systems. Your user name and password are the means by which the system identifies you. One of your responsibilities under the Security Rule is to properly manage your password and keep it secret. You should not have your password in a place that someone else could access it (e.g., openly displayed in your work area). Never allow someone to log into the system under your credentials or allow another person to do work in the system under your login. Any work done under your credentials will be attributed to you, and the system has no way to identify work that another person performed under your login. You would be held responsible for anything another person does under your credentials.

You must also comply with requirements to change your password periodically. Your software might automatically prompt you to change it, or there might be a policy in place that requires you to change your password on a periodic basis. You must adhere to complexity requirements for passwords as defined by your organization. If you become aware that your password or other authentication credential has been compromised, report it immediately to the Security Officer/designated individual.

e-Compliance Training Test

HIPAA Security Rule - May 2021

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 Integrity controls refer to measures which ensure that EPHI is not improperly altered or destroyed.

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

2 Once you have been granted permission and credentials to log on to your organization's systems, you may access any EPHI because you're an authorized workforce member.

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

3 In a phishing scheme, an attacker gains access to your network through an open port.

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

4 Even if your organization has a presence on a social media platform, and even if a patient reaches out via social media, you should never publish any EPHI on a social media site/ platform.

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

5 Password management requirements include safeguarding your password, changing it when prompted and following password complexity requirements.

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

6 You should not allow another individual to log into the system under your credentials or allow another person to do work in the system under your login.

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

7 The "minimum necessary" concept requires that your organization limit the number of users that access EPHI.

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

8 Authorized users may connect outside media, such as cell phones, to the network to charge them.

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

9 Common examples of security incidents include, but are not limited to, sharing a password, failure to report known security incidents, bringing in outside media and connecting it to the network without having it scanned or approved, and failure to follow proper protocols for securely transmitting EPHI.

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

10 Under login monitoring, users may get locked out of systems after a specific number of unsuccessful attempts.

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

Click Here to Take Your Quiz