e-Compliance Training

HIPAA Security Rule - May 2020

THIS TRAINING SESSION IS RECOMMENDED FOR:

All members of a healthcare organization's workforce. This includes employees, contracted staff, volunteers, interns, residents, and students with access to your information system, etc.

Training Objectives

The objectives of this training module are to:

- outline Security Rule standards;
- identify risks to electronic protected health information (EPHI) and responsibilities for workforce members;
- communicate requirements for protection from malicious software, login monitoring and password management;
- identify reporting requirements for security incidents; and
- explain disciplinary action that would be imposed for non-compliance.

An organization is responsible for all EPHI it creates, receives, maintains, or transmits, regardless of its origin, storage location, etc. The Security Rule applies to all media, devices, equipment, etc. that stores electronic protected health information (EPHI) and includes a variety of administrative, technical, and physical security procedures for covered entities to use to ensure the confidentiality, integrity, and availability of EPHI. The Security Rule addresses the fact that an increasing number of processes in practices are accomplished via electronic means, increasing the risks to EPHI.

The Security Rule is flexible and scalable, meaning no two organizations will comply the exact same way, and there are no specifically required software programs—many different programs could be used to achieve a certain measure. Other considerations include the size and complexity of your organization, infrastructure, costs, and likelihood and possible impact of the risks to EPHI. There are many different methods/software programs/mechanisms that may be used to meet the standards within the Rule.

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 a security official who is responsible for developing and implementing its security policies and procedures. Find out from your supervisor who has the role of Security Officer for your organization.

Information Access Management - Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," 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 (role-based access). Because of this requirement, you will likely have a privilege set in the electronic systems such as the EMR/EHR and practice

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.

management systems. That privilege set allows you to perform/access only the things needed to accomplish your work duties.

Workforce Training and Management - A covered entity must provide for appropriate authorization and supervision of workforce members who work with EPHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures. This means that you will be subject to disciplinary action (sanction) if you fail to follow HIPAA policy 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 - A covered entity must 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.

Workstation and Device Security - A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place 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

A covered entity must implement technical policies and procedures that allow only authorized persons to access EPHI. Your login grants 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 - A covered entity must implement hardware, software, and/or procedural mechanisms to 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 may use that ability to investigate instances of suspected improper access, etc.

Integrity Controls - A covered entity must implement policies and procedures to ensure that EPHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that EPHI has not been improperly altered or destroyed. Your IT person/vendor will have implemented several different mechanisms to help ensure integrity of data.

Transmission Security - A covered entity must implement technical security measures that 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 remote in to your network.

Security Incidents and Sanctions

You will receive security reminders, initial and annual training on security, and instruction on policies and procedures. Your practice will identify what would be considered security incidents or violations of its security policies and procedures. 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.

If you fail to comply with your practice's security policies and procedures, you will be subject to disciplinary action, also known as a sanction or penalty. Sanctions 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, absent aggravating or mitigating circumstances.

Minimum Necessary Standard

The minimum necessary standard is a concept that applies both under the Privacy and Security Rules, and requires that you only access, use and disclose patient information that is needed for you to perform your job 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. Check with your HIPAA compliance officer for more information on any exceptions that apply.

Awareness Requirements

There are three specific awareness items with regard to HIPAA Security: protection from malicious software, login monitoring and password management. You play a role in helping to ensure the security of EPHI.

Protection from Malicious Software - Malicious software can take many forms. Malware can be a computer virus, disruptive code, ransomware, which locks up 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, still use caution, 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 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 use caution in visiting web sites, and your practice may have installed web filtering software that prevents you from visiting certain sites. Your practice may also have a policy that requires you to limit web site usage to those that are required for your job duties.

You should never bring in outside media and 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, and it could migrate to the practice's network 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 practices 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 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, along with other steps. Be sure to have these steps handy to ensure you are able to take quick action.

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 look exactly like those from 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 caution when opening email messages. If, after opening, you suspect it may be a phishing attack, do not click any links. Check the sending email address. 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.

Login Monitoring – Monitoring your login process presents an opportunity to alert your practice to a potential security issue within your information system. When you start up a computer and access your practice's network and/or the EHR/EMR/practice management systems, you are required to log in or verify that you are part of the practice's workforce. 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 practice's 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 be aware of any unusual behavior, errors, or alerts that occur. If you receive an alert or error message, immediately notify a supervisor, 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 – Your user name and password are the means by which the practice's 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). You should also 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.

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.

Social Media and Acceptable Use Policies

Your practice will have established rules for proper use of your workstation, including sites you may visit on the Internet. Further, your employer may outline permissible use (if any) of social media. It is critical that you never publish any EPHI on social media, even if a patient reaches out via social media requesting information. You would always reply via a private method such as phone, encrypted email, a patient portal, etc. in response to an inquiry via social media, if EPHI would be needed in the reply. Recent breaches and potential data mining from social media increase the need for vigilance.

e-Compliance Training

HIPAA Security Rule - May 2020

F

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 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 access the data again.

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

2 When logging in, you should 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.

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

3 It is ok to reply to a patient on a social media platform if the patient initiated the communication via public means.

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

4 The Security Rule only covers EPHI stored in your EMR/EHR or practice management software.

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

5 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**

6 It is ok to share your login/password with another staff member as long as he/she is already an authorized user of the system.

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

7 Your Security Officer has the ability to track your activity within systems, and may use that ability to investigate instances of suspected improper access, etc.

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

8 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.

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

9 Once you confirm that you know the sender of an email, it is ok to open any attachments.

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

10 The Security Rule is flexible and scalable, meaning no two organizations will comply the exact same way, and there are no specifically required software programs—many different programs could be used to achieve a certain measure.

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

Click Here to Take Your Quiz