e-Compliance Training

HIPAA Security Rule - May 2022

THIS TRAINING SESSION IS RECOMMENDED FOR:

HIPAA's Security Rule requires that annual retraining be completed by 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 safeguards and responsibilities for security of EPHI;
- provide annual retraining on protection from malicious software, login monitoring and password management topics;
- identify the need to prevent and report security incidents; and
- explain disciplinary actions.

HIPAA's Security Rule applies to all electronic protected health information (EPHI), regardless of its location. This includes any device, media, hardware, software, component, etc. that is connected to your network, or that stores or transmits any EPHI. There are a variety of administrative, technical, and physical security safeguards to implement that will ensure the confidentiality, integrity, and availability of electronic protected health information (EPHI).

The Security Rule is flexible and scalable, and the measures selected to secure EPHI are dependent on the size and complexity of your organization, infrastructure, costs, and likelihood and possible impact of the risks to EPHI. The Rule does not require use of any particular software or method to meet the requirements. For example, your organization may choose from a large variety of services to protect data during transmission, ranging from encrypted email vendors to secure file sharing services and secure patient portals.

Required Annual Retraining

There are three required areas of awareness/training within HIPAA's Security Rule:

- 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 through 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.

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.

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 or devices nor connect them to your computer/network without approval from your Security Officer. Outside media/devices include CDs, DVDs, flash drives, removable hard drives and even cell phones. Cell phones can be infected with malware, which could migrate to the information 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 prohibit 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 from your workstation to others on the network. 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, re-names 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 the 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 can take quick action in the event of a malware incident. Some steps that may seem desirable, such as preemptive password resets, may alert the intruder that you are aware of their presence. Always follow the instruction of your Security Officer.

If you have been asked to run 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.

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, contact your Security Officer for next steps or follow procedures that have been communicated in advance.

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 as an authorized user. 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. Since there is no way for the system to differentiate work that another person performed under your login, you would be held responsible for all of it including errors, negligence and malicious acts. If you become aware that your password or other authentication credential has been compromised, report it immediately to the Security Officer/designated individual.

You must adhere to password complexity requirements as defined by your organization, such as for a minimum number of characters. In addition, your software might automatically prompt you to change your password on a periodic basis, or there might be a policy in place that requires you to do so, the frequency of which is determined by your Security Officer/management. A different password should be used for each log in, such as for access to a network, EMR/EHR, PM system, secure portals, etc.

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. Use of invalid login credentials will result in a denial of access, and the system should only allow a limited number of attempts before the user gets locked out. The 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, or from using an automated password spraying program.

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.

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 to meet this requirement.

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 serves as the Security Officer for your organization if you've not already been informed.

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 organizations are so small that global access privileges are needed for users who are cross-trained. Even then, admin-level privileges are generally not granted to all 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. This requirement is usually met through performance of a security risk analysis and technical network assessment.

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, alarm code, etc.) will be granted it, and if you've been assigned a means of access, that fact will be documented.

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 or activate a screen lock if you know you are walking away from your station/leaving it unattended. 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 to your workstation, the network, the EMR/EHR and practice management systems, as appropriate. As previously mentioned, your login should be 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 information systems 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 program or Virtual Private Network (VPN) for anyone who needs to remotely access data on your network.

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

Common examples of security incidents include, but are not limited to, sharing passwords/credentials, 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.

It is your responsibility to avoid causing security incidents, and to immediately report any security incident of which you become aware, whether you caused it or simply discovered it. If you make a report in good faith, your organization may not take any retaliatory action against you, although you may be subject to disciplinary actions in certain circumstances (such as knowingly failing to follow established procedures).

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). Sanctions will be applied equally to all workforce members, regardless of rank or position, unless there were aggravating or mitigating circumstances.

Minimum Necessary

"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. Check with your HIPAA compliance officer if you have questions about the minimum necessary standard.

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 you may be provided with information in an employee handbook. In addition, your network may have security settings in place that may block certain web sites from loading at all. You may only be able to access web sites that are necessary to perform your duties.

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 or complaint, if EPHI is necessary in the reply. Recent breaches and potential data mining from social media are cause for increased vigilance.

e-Compliance Training Test

HIPAA Security Rule - May 2022

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 Patient portals, secure email systems and secure file sharing programs are sometimes utilized to protect EPHI that is transmitted over an open electronic network.

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

2 "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, with certain exceptions.

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

3 If you know your workstation will be unattended for a time, you should log out or activate a screen lock.

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

4 When a patient contacts you via social media, it is permissible to reply with PHI if needed, because the patient initiated the contact.

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

5 Lockout protections (when a user gets locked out after repeated unsuccessful attempts to log in) help ensure that only authorized individuals are accessing EPHI and prevent an unauthorized person from trying to guess at a password, or from using an automated password spraying program.

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

6 Portable media and devices such as flash drives can transmit malware, and are sometimes prohibited, or if permitted, must first be scanned and/or approved for use.

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

7 The Security Rule requires that all organizations utilize key fobs or key cards for access instead of regular locks and keys, because each user's actions can be identified.

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

8 Audit controls mean that your Security Officer has the ability to track your activity within information systems to investigate suspected improper access, errors, etc.

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

9 Mobile devices require security measures, but the Security Rule allows for flexibility in how those measures are implemented.

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

10 Under the Security Rule, users must pass a background check prior to being granted access to systems the store or transmit EPHI.

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

Click Here to Take Your Quiz