Cyber Education is More Than a Meeting

By Rana McSpadden, FACMPE

A practice does not need to implement the most expensive technology or hire full-time IT staff in order to comply with the HIPAA Security Rule. So long as policies and procedures, technology, and physical safeguards which are appropriate for the size of the practice are put in place, compliance is achievable. However, if staff members are not trained in their role in the prevention of cybersecurity incidents, all other prevention measures may be for naught. Staff are on the front lines of cybersecurity and, without the proper knowledge and skills to recognize risks, may leave themselves and the practice vulnerable. Firewalls cannot prevent hackers from accessing systems if staff members inadvertently give them their login credentials or download malware through infected links sent through a phishing email. Device encryption is futile if staff members do not log out of the system before walking away from their workstation or laptops, allowing someone to walk up and access anything in the system.

In addition to HIPAA privacy education, security awareness and training should also be

provided to all members of a practice's workforce.

Who should receive education?

Every member of the practice workforce should receive education. This includes staff, management, and providers. Anyone who has access to the practice's systems, including any temporary staff or students, should receive education on their role in preventing cybersecurity incidents.

How often should education be provided?

As with general HIPAA education, all new workforce members should receive education as soon after hire as possible. Additionally, re-education for all members should be performed on a periodic basis as well as when there are changes in policies and procedures, whenever new software or hardware is implemented, or if changes are made in the Security Rule. It is best practice to do security awareness training at least annually. Educational calendars are an easy way to stay abreast of training and provide reminders. To supplement and reinforce education efforts, the security reminders and updates should be provided periodically throughout the year and whenever there is a security incident. These reminders should be brief and provide timely information regarding security risks to the practice.

What should be included in education sessions?

Some of the most important topics that should be covered in cybersecurity education relate to ways in which workforce members can guard against, detect, and report malicious software. Topics include (but are not limited to) how to spot a phishing email, the risks of clicking suspicious links, the dangers of downloading infected files, and to whom to report suspicious activity. This point of contact may be the HIPAA Security Officer, a manager, or IT personnel. Additional education may focus on processes or software used to report suspicious emails or activity. Other topics may include information about various threats to practice systems and why they are a threat, such as ransomware. Additionally, workforce members should be educated on log-in monitoring to thwart inappropriate log-in attempts, what happens when there are too many log-in attempts, and how to manage passwords. Password management education should discuss the use of complex passwords, how to change passwords and how often passwords should be changed, as well as the dangers of keeping written passwords in the open or sharing them with others. A practice's security policies and procedures may provide a good place to start for an outline of topics to cover, as well as providing some of the content to be presented.

How should education be provided?

There are several ways to provide cybersecurity education and reminders to all members of the workforce. Full education can be provided through formal educational presentations or webinars. Routine security reminders can be provided using memos, postings in employee areas, email blasts, newsletters, or during monthly staff meetings. Whatever

format is used, it should be what benefits the practice and workforce most. As with other areas of a practice's HIPAA compliance program, retain documentation of education efforts, including the content presented, date presented, presenter information, and to whom it was presented. To assist with practice education needs, SVMIC provides multiple resources on our website as well as through Cybernet. To access these resources, click here. If you have questions about cybersecurity or access to these resources, call 800-342-2239 or email Contact@svmic.com.

If you experience a cybersecurity incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak with the Claims department.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage account here.
