Cybersecurity, HIPAA-compliant communications

Q What are some measures to take to lessen the risk of a cybersecurity attack on a practice and patient data? In the event a cybersecurity attack does happen, what are some next steps to take?

A In general, there are a few different things that can be done to help protect a practice from a cybersecurity attack. According to the U.S. Department of Homeland Security, 96 percent of cybersecurity breaches could have been avoided with simple or intermediate controls.

As a best practice, passwords should be strengthened, suspicious emails should be screened, clicking on suspicious links should be avoided and anti-virus software should be installed.

A plan should be in place in the event a cyberattack does occur, and practice employees should know who to contact and what to do next. Breaches of unsecured protected health information should be reported to affected individuals/patients, the U.S. Department of Health and Human Services and, in some cases, to the media (this varies state-to-state). As a best practice, legal counsel should be contacted to ensure all appropriate steps are being taken.

Q How can a practice remain HIPAA-compliant with its communications – including mobile device communications – to patients?

A In general, any and all patient identifiers should be removed, communications should be kept general, minimal necessary information should be conveyed and patient consent for digital communications should be sought in advance.

When using mobile devices, passcode protection should be enabled. Mobile devices should be encrypted. Mobile devices should access only a specific Wi-Fi connection established for the mobile devices. Each mobile device should be registered with the practice/organization. Also, all mobile device software and applications must be current and updated.

Q What additional information is available for cybersecurity guidance and HIPAA Security Rule compliance?

A Cybersecurity guidance and a checklist of helpful information are available on the HHS.gov website. This information is designed to give HIPAA-covered entities and business associates insight on how to respond to cyber-related incidents.

The cybersecurity checklist and infographic explain these steps in brief. If a practice experiences a ransomware attack or another type of cyber-related incident, first steps include executing response and mitigation procedures as well as contingency plans.

Next, the entity should report the crime to criminal law enforcement agencies. The entity also should report all cyber-threat indicators to the appropriate federal agencies and information-sharing and analysis organizations. (See HHS.gov for more information on these types of organizations.)

Finally, the breach should be assessed to determine if there is a breach of protected health information.

Additional information and next steps for handling a breach are available at HHS.gov/HIPAA/for-professionals/security/guidance/cybersecurity/index.html. ■