Do These 5 Things Now to Mitigate Your Cyber Exposure

Sterling Seacrest Pritchard

1. Use both a Virtual Private Network (VPN) and Multi-Factor Authentication (MFA)

The HIPAA Security Rule requires medical practices to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. One way to do so is through the use of a VPN for all devices used in your practice. A VPN encrypts traffic between two devices via a secure tunnel, making data unreadable for would-be cyber criminals. VPNs work for mobile devices too, regardless of whether you are connected to Wi-Fi or using cellular data. A corporate VPN (connecting the user back to the office network) is recommended over a consumer VPN which may encrypt your traffic but does not provide the same connection back to the office.One vulnerability of VPNs, however, is the entry point where users log in to the network. If the user's ID and password have been discovered by a cybercriminal (e.g., a remote employee's personal computer was unknowingly breached), that criminal can access data through the VPN. Therefore, you also need MFA in place which requires the employee to then verify their identity – a second layer of protection. In fact, if you check your cyber liability policy application, you were probably asked to confirm that everyone uses VPNs and MFAs.

2. Backup your medical records

The HIPAA Security Rule requires medical practices to establish a data backup plan whereby procedures are implemented to create and maintain retrievable exact copies of electronic protected health information. A good rule of thumb to follow is the "3-2-1 approach" which means: "3" - Create three copies of data; "2" - store them on at least two different media; and "1" - have one copy stored securely offsite. In fact, best practice is a "3-2-1-1-0 approach" which requires one backup to be completely isolated/offline ("air gapping") with "0" errors with the backup. With air gapping, computer systems and networks are not connected to other devices and networks, and since it is disconnected, a cybercriminal will not be able to access your data.

3. Never save passwords in mobile devices or web browsers

Whenever you create a new online account, you have likely noticed a pop-up window asking if you want to save the password in your browser. Do not do it. If a cybercriminal gains access to your computer or mobile device, they can easily access all of your saved passwords. Moreover, if your browser is corrupted, cybercriminals can remotely access your passwords, compromising all of your accounts. That said, you also do not want staff writing down passwords on sticky notes and pasting them to the sides of their desktop computers. Best practice is to use a password manager which is a software application designed to store and manage online credentials and generate passwords for storage in an encrypted database and locked behind a master password.

4. Understand and address the use of mobile devices (smart phones, iPads, laptops) by staff

The 2022 Verizon Mobile Security Index annual report found that 45% of respondents said their organization had been subject to a security incident involving a mobile device that led to data loss, downtime, or another negative outcome. With the proliferation of mobile devices in healthcare, it is imperative, therefore, that you take certain steps to mitigate your cyber risks relative to the use of such devices, including: (i) registering all mobile devices with the organization and providing authorization, where warranted, to access PHI; (ii) requiring password/pin protection or biometric authentication on mobile devices to restrict access to sensitive patient data to authorized users; (iii) encrypting data on the mobile devices; (iv) requiring use of a secure messaging app specifically designed for mobile healthcare communication; (v) ensuring that all security updates are downloaded as soon as they become available; (vi) again, ensuring staff never uses public Wi-Fi networks without going through a VPN; (vii) only plugging the mobile device into a secure system, like a home computer; (viii) installing and utilizing a "remote wipe" function on all mobile devices allowing you to erase all patient data from an employee device if it is lost or stolen; (ix) installing firewall and anti-malware protection on all devices; and (x) training staff on mobile device management, privacy, and security.

5. Limit or forbid the use of personal computers in the workplace

Once an employee uses their own personal computer for work, you lose your ability to adequately protect the practice against cyber-attacks because employees likely (i) do not have the level of anti-malware software on their personal computer that is mandated in the office, (ii) have an older operating system that is vulnerable to attack, and/or (iii) have failed to update their software with security patches. Moreover, they may not use encryption or have a remote wipe feature installed, or they may inadvertently store PHI to their hard drive. Also, when the employee leaves the practice, the employer is unable to remove any PHI that may be stored on their computer.

Please Note: SSP is not a law firm, and our recommendations should not be construed as, nor are they intended to be, legal advice. SSP encourages its clients to consult with legal counsel and/or other professionals about the information contained in this communication.

2024 © Sterling Seacrest Pritchard, Inc. | sspins.com