COMPUTER, LAPTOP & MOBILE DEVICE SECURITY

Sterling Seacrest Pritchard

What is it and what's required:

The HIPAA Security Rule requires medical practices to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. A big part of this requirement is securing remote access (whether at home or on the road) from a home computer/laptop or mobile device. A recent survey performed by Bitglass data protection company found that:

- 68% of healthcare data breaches were due to the loss or theft of mobile devices or files.
- 48% of data lost was on a laptop, desktop computer, or mobile device.
- 23% of cyber breaches resulted from hacking not connected directly to the loss or theft of a mobile device.

Steps toward compliance:

1. Perform a comprehensive HIPAA Security Risk Assessment looking at what, where, when, and how, your staff accesses e-PHI.
2. Secure all electronic devices (internal and external) with firewalls and anti-malware protections and apply software updates/patches immediately, including regular updates of anti-virus and anti-malware software. This needs to be done globally on all devices and checked on a regular basis. Note: Vulnerabilities - for which updates and patches are designed to correct – on average take only two weeks before a cyber-criminal takes advantage of them.
3. Remove End of Life (EOL) operating systems, software, and applications. EOL systems are those that are no longer supported by the vendor/provider and do not receive product updates and security patches.
4. Use strong passwords and change them every 30 days. Don't use obvious, easy-to-guess passwords, don't use the same password on multiple websites or systems, and don't share your password with anyone else. Use a password manager on all devices.
5. Enable encryption of all devices and storage - this can be accomplished on iOS, Android, macOS, and Windows.
6. For EHRs, (either on the cloud or onsite), encrypt network access to these applications. Software applications that encrypt data prevent hackers from accessing sensitive data, usually by requiring a "key" to encrypt and/or decrypt data.
7. Register all mobile devices with the organization and install a "remote wipe" function on each which allows management to erase all patient data from an employee device if it is lost or stolen.
8. Set your device to lock (go to a password-protected screensaver) after a short period of non-use.
9. Ensure physical security of all mobile devices (e.g., don't ever leave phones, laptops, etc. in your car - take them with you).
10. Secure your network connection through use of a VPN service (it will encrypt all of your internet traffic) with Multi-Factor Authentication (MFA). A VPN should be mandatory if using public Wi-Fi.
11. Audit the use of remote access software that is installed on endpoints to ensure they remain in use. Check to make sure that MFA is enabled on software applications and operating systems.
12. Secure your data – Best practice is to work with data stored in a secure cloud service. Never download or copy data to your device's local storage.
13. Encrypt all emails - Never put confidential data on an unencrypted flash drive or portable hard drive. Change your browser settings so the browser's data cache (stored data from your session) is wiped each time the browser is closed.
14. Carefully examine any links to ensure the destination is correct with no misspellings and consider if you were expecting a link from the sender, and as an extra layer of protection, consider installing content filtering. Then test staff for compliance with a mock phishing test such as the one provided by KnowBe4© (see https://www.knowbe4.com/phishing-security-test-offer).
15. Encourage staff to report breaches and unusual activity immediately.
16. Consider using email filtering through your email provider (e.g., Microsoft 365, GSuite, etc.), or you can use a 3rd party for a more robust experience.
17. Develop a policy that incorporates all of the above.

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