TPCA TENNESSEE PRIMARY CARE ASSOCIATION

Cybersecurity Best Practices

A strong IT infrastructure with a focus on cybersecurity is essential in healthcare for many reasons. The protection of patient data, compliance with regulations, prevention of data breaches/ransomware attacks, the security of medical devices, maintaining continuity of care, and building trust with our patients are all of paramount importance. Within your organization, the following should be standard practice as part of your cybersecurity workflows:

Establish a Security Culture

Overcome the perception in your organization that "it can't happen to me". Cyber threats are everywhere and our workforce is our most critical tool to preventing bad actors from infiltrating our systems to gain access to sensitive data.

Promote Good Computer Habits

Like we share with our patients what the best habits are for a healthy and happy lifestyle, we must do the same with how we use our technology. Keep your technology up-to-date, running properly, and well maintained to avoid security vulnerabilities and performance issues.

Antivirus Software

Every computer, mobile device, and server needs to be protected within your organization at all times. Ensure that you antivirus software is fully compliant, up-to-date, appropriately implemented throughout your IT environment, and monitored at all times.

Monitor Access to PHI

Protect your patient's data along with who accesses it and how. Keep track of who in your organization has what level of access to this data and why.

Control Network Access

Monitor, at all times, who is accessing your network and why to properly protect your sensitive data.

Protect your Mobile Devices

While portability increases convenience, these devices are more likely to get lost, stolen, or have their data corrupted. Every mobile device in your organization must be encrypted to ensure it is secure and all of its data is protected regardless of the situation.

Use a Network Firewall

Adequate protection for your systems that are connecting to the Internet, including your EHR, are critical for preventing threats and intrusions from malicious sources. These bad actors will hold your data for ransom once they are able to access it.

Plan Ahead

Expect the unexpected! Implement Security Risk Assessment (SRA) Tools and Penetration Tools that can tell you where your system vulnerabilities exist. Draft downtime procedures that will keep your clinic operational if your IT systems go offline. This includes the reporting of the event to the proper authorities.

Strong Password Complexity

Passwords are critical to protecting information and their complexity is equally as important. Make sure to use guidelines that include at least 8 characters and not usual words of phrases as part of your passwords.

Control Physical Access

Increased access to physical equipment makes it more likely for data to be compromised or stolen. Always log who has physical access to your systems, why and how.