Healthcare Cyber-Security Best Practices to Protect Vital Patient Data

In recent years, hackers have turned their attention to healthcare organizations. Not only do hospitals store valuable personal data, but they often underspend on cyber-security. This makes them highly attractive targets. Investing in solid healthcare cyber-security protects essential data and ensures regulatory compliance. More importantly, it can quite literally save lives.

Late last year, East Ohio Regional Hospital discovered a ransomware attack. Thanks to multi-layer defense systems and reliable backups, the hospital managed to recover with minimal damage. Other hospitals around the country have not proven so lucky. From disruption of services to exposure and loss of critical patient data, the costs can cripple an organization.

Attacks will happen. However, implementing security best practices like the following helps to ensure that when an attack occurs, your organization can recover quickly.

Backups, Backups, Backups

In the event that your organization suffers a ransomware attack, your most important recovery tool lies in having reliable backups. Run backups frequently and store them off-site. Test your backups. You cannot afford to find out too late that your backup files have become corrupted and that you have lost months of patient data.

Multi-layered Defense

With a backup plan in place, you can focus on building a defense in depth strategy around your information assets. Start with updated antivirus and anti-malware programs on all servers and computers. Ensure physical security, preventing access to computer equipment. Add strong firewalls, solid password procedures for all devices and advanced threat detection.

Regular Security Audits

Conduct regular security audits to reveal any vulnerabilities in the physical systems and the network. Audits should also cover exposure to the internet and any connected devices, as hackers can use these as entry points.

In addition, remember that any third parties that have access to your system provide a convenient back door to sensitive data. Make sure that these vendors follow minimum security standards and include them in regular audits. This includes cloud services providers that may store your data offshore in countries not bound by the same data protection laws.

Remember the Human Factor

With all the security technology at our fingertips, the weakest link in our defense remains the human element. Most security breaches occur because of human error. An employee clicks on a link that looks almost legitimate or neglects to secure his laptop with a strong password. Another employee sends sensitive information through unsecured email.

Implement comprehensive but easy to follow security practices, including email policies. Conduct regular training for employees to make them aware of policies and help them practice safe computing. Teach them to recognize the early signs of an attack and know how to respond.

Encryption

Make sure to encrypt all sensitive data both in transit and at rest. This includes email encryption, as well as encrypting data in its storage place on hard drives or in the cloud. While encrypting data will not prevent an attack, it can prevent hackers from using the data once they access it.

Security Strategy for Mobile Devices and IoT

With the prevalence of mobile computing and the Internet of Things (IoT), hackers have a much broader surface to attack. Many organizations include bring-your-own-device (BYOD) policies. Because a lost smartphone or stolen laptop can quickly result in a serious data breach, be sure to implement comprehensive mobile device management.

Likewise, medical devices from insulin pumps to wearable monitors now often include internet connectivity, making them vulnerable to attack. Review vendor cyber-security practices, keep up-to-date on any software and hardware fixes and carefully manage access to those devices.

Continuous Monitoring

Like any potentially serious condition, healthcare cyber-security benefits from continuous monitoring. Whether through in-house IT resources or through a managed services provider, set up automated monitoring of your network.

Monitoring systems learn the patterns of each user on the network and can quickly identify anomalies. For instance, if activity in a user account deviates significantly from the norm, the monitoring program will alert IT. At the same time, the system will prevent further action from the user without proper authentication.

Enlist a Trusted Partner to Ensure Healthcare Cyber-Security

We know that as a healthcare organization, you focus on saving lives. We can help you implement the comprehensive healthcare cyber-security that makes that possible. The security professionals at Messaging Architects have worked with healthcare organizations of all sizes to implement multi-layered security that ensures the safety and privacy of critical data assets.