2018 Cybersecurity Outlook

Looking ahead to 2018, cybercriminals will redouble their efforts to steal personal health information (PHI). The number of ransomware attacks has steadily risen for the last few years, and there is no indication that it will slow anytime soon. Reliance upon technology in healthcare continues to grow, providing cybercriminals more means to access more data. By its very nature healthcare is more susceptible to cybercrime than other industries. There is some good news, however; with education and the right resources, today's physicians and their practices can be better equipped to prevent a security breach or handle one should it occur.

The healthcare industry is particularly vulnerable to cyberattacks for a number of reasons. One example is the use of mobile devices by doctors, such as phones and tablets, which contain and manage patient data. According to Adi Sharabani in his article "Mobile Security Trends in Healthcare" on Skycure.com, 65% of physicians send PHI via text message, and over 70% of physicians were using a mobile device to aid their practice as of 2015. Certainly, these numbers are higher in 2018. These devices are not only easier to lose or have stolen, but when they are offsite, many of the security measures provided by a secure in-office network do not protect them.

Like everyone, the healthcare industry is becoming increasingly reliant on technological devices. From insulin pumps delivering a steady stream of insulin to diabetics and wearable trackers monitoring blood pressure and heartrate, to a radiologist in Australia reading the radiograph of a patient in East Tennessee, technology utilization has burgeoned over a short period. For many people, it is difficult to imagine life without these conveniences. Nevertheless, the devices and technologies we use constantly are all vulnerable to cyberattacks that could put them out of commission.

While cybercriminals continue their targeted and increasingly sophisticated attacks on the healthcare industry, physician practices can get smarter and more prepared. Some of the ways to be better equipped to prevent a cyberattack in 2018 are:

1. Back up your data - the more frequently the better
2. Protect your equipment offsite as well as onsite
3. Offer multiple training courses for employees in order to keep them aware of the evolving tools used by cybercriminals
4. Do not become complacent with security and authorization procedures
5. Update your hardware and software when updates are available
6. If you do fall victim to a breach, promptly notify the affected parties.

Lastly, even when you do everything you can tactically to secure your data, it is best to have cybersecurity insurance to protect your practice – just in case.

SVMIC's medical professional liability policy includes $50,000 of cybersecurity coverage with NAS to assist in mitigating the damages associated with a security breach. Using SVMIC's website, policyholders can access multiple online resources, which provide tools such as monthly cybersecurity updates, webinars and online training and support. In addition, SVMIC's Medical Practice Services offers consulting and training related to cybersecurity and HIPAA.
