With Rising Cyberattacks on Healthcare Orgs, these 4 Things Need to Change

Even though stories of cyberattacks regularly flood our newspapers and national broadcasts, the last place anyone expects the next debilitating security incident to hit is their family doctor's office. Unfortunately, small to midsize healthcare organizations are exactly where cybercriminals have been targeting more often in recent years, especially since COVID-19 hit. Just within the last six months, attacks on medical facilities globally have spiked an additional 45 percent of an already escalated rate since 2019. Incredibly, that is more than twice the increase in cyberattacks of any other industry during the same period.

One might assume a major uptick like this would have every medical practice investing heavily in security infrastructure to protect their practice and patients' electronic private health information (ePHI). As it turns out, that assumption would fall flat because more often than not, healthcare organizations do the bare minimum to protect themselves. This trend is a major problem considering over 90 percent of SMBs that get hit with a malware attacks close within one year. In order to understand the disconnect between medical practices and essential cybersecurity measures, further examination is necessary.

Why Healthcare is so Vulnerable

As recently as 2014, the biggest threat to PHI was still the physical theft of paper records which demonstrates medical practices' relatively slow adoption of IT infrastructure. The passage of the 21st Century Cures Act in 2016 which creates transparency for patients to access their own healthcare information helped to spark a substantial migration from paper records to electronic health records (EHRs). However, ensuring interoperability and information sharing has made much of the infrastructure already acquired by medical practices outdated and a scramble to comply has led to a mixed bag of solutions, too often without the help of IT experts. That leads to a cybersecurity nightmare

with untrained staff trying to utilize various systems, any one of which could lead to a security incident or worse, a full breach. These vulnerabilities would be less impactful if not for the increased targeting of medical organizations by cybercriminals in the last two years.

Why are cyberthieves targeting healthcare businesses to begin with? In practices large and small, cyberthieves have found a gold mine for several reasons. Obviously, the ease of which they have been able to access unmonitored outdated platforms is the predominant factor, as illustrated above. When a cyberattack is successful, thieves gain access not only to operational information but to patients' ePHI. These records can contain names, DOBs, social security numbers, health insurance cards, as well as private health and genetic information. Because this data is regulated by HIPAA, cybercriminals know medical practices are likely to pay a high price to recover it, thus the term ransomware. This accounts for the fact that 91.2 percent of medical breaches have led to stolen ePHI and the increased publishing of personal data.

Another pain point in need of attention is when Covid-19 hit, healthcare organizations were suddenly distracted with a major pandemic and hackers saw an opportunity to exploit the chaos. With administrative staff working more from home and some moving to part-time hours, security and training became even less of a priority. Consequently, phishing emails have become the main entry point for ransomware attacks which can be complicated by other factors like appropriate permissions that allow criminals to move laterally throughout infiltrated systems. That leads to difficulty detecting a breach and longer recovery times thereafter.

To make matters even more dire, healthcare leaders have largely accepted the false notion that a solidly secure environment is unattainable. While it's true that it is complex and often requires outsourced expertise to understand various platforms thoroughly enough to secure them, it is possible to minimize your risk and protect your practice. Another assumption that limits cybersecurity efficacy for some organizations is the belief they are too small to be targeted by hackers, which couldn't be more contrary to the data. In LightPoint, you have a partner to cut through the noise and help you design a security plan that meets the needs of your practice.

To Secure Your Business…Start Simple

While the process of preventing ransomware attacks is complicated, getting started doesn't have to take over your entire work life. There are a few common missteps that healthcare practices routinely make and starting with those will get you on the right track to secure your IT environment.

1. **Don't Rely 100% on HIPAA Guidance** - While you must, of course, remain compliant with HIPAA and follow their guidelines to avoid stiff penalties, they were written 25 years ago and are outdated. No one writing these regulations could have imagined at the time concepts such as cloud migration and interfacing electronic health records as we know them. There is a requirement for "regular" risk assessments to secure your PHI which most experts interpret best practices as taking place annually, and that is good advice. That said, even if you fulfill this basic obligation, HIPAA doesn't provide any clear guidelines for what to do with the information once you have it. This leaves medical practices guessing without a clear map and can lead to devastating wrong turns down the line.
2. **Stop Skipping your Risk Assessments** - Last year, the Department of Health and Human Services Office for Civil Rights (OCR) released an audit report for the healthcare sector on HIPAA compliance from 2016-2017. Among several alarming findings, it showed that a majority of medical organizations were failing to run risk assessments as required by HIPAA. That means that, not only were they deficient in the regularity of their risk evaluation efforts, but most practices weren't doing them at all. This decision leaves your business extremely vulnerable. With the rise of cybercrime against small practices, you are essentially a sitting duck for ransomware attacks and lost ePHI. Even if you are able to pay the ransom and somehow squeak by with your business intact, the massive HIPAA fines may just finish the job.
3. **Don't Try to Handle Risk Assessments In House** - A comprehensive risk evaluation takes many hours to do properly and demands significant expertise. Our LightPoint methodology takes a deep dive into three main areas of your practice: technical, physical, and administrative. The technical review looks at all your systems and devices to identify any technological weaknesses while the physical section has more to do with security alarms, cameras, location of servers, and other concrete security vulnerabilities. Our administrative evaluation dissects your hiring practices, background checks, training, policies, as well as your recovery plan in case of an attack. Considering many security failures begin with a phishing campaign or some other avoidable misstep, risk assessments must be professional and thorough.

4. **Start Implementing Expert Recommendations** - For those healthcare practices that actually do adhere to the HIPAA risk assessment requirement and hire an outside company to conduct a complete annual review, most do not follow the advice. This is where the lack of HIPAA guidance really becomes a problem because without specific security regulations in place, healthcare leaders may feel a lack of urgency when in fact, nothing could be more critical. Unfortunately for those who dismiss the advice and eventually endure a security breach of ePHI, having the risk assessment done alone will not save them from debilitating fines. LightPoint offers a risk management plan as part of our evaluation process which gives tangible steps to take to secure your environment. Those practices that adhere to expert advice are far less likely to experience a breach.

Final Thoughts

When all is said and done, making the decision to fight back against future cyberattacks not only protects your business, but the lives of your patients as well. Stolen ePHI can lead to a nightmarish reality for victims with identity theft, fraud, or even the publishing of embarrassing images. Fortunately, you have more control over securing your healthcare environment than you may realize. Partnering with a reputable Managed IT Provider can help you understand what your vulnerabilities are and how to approach them. Following the basic HIPAA guidelines requiring risk assessments is a great start and a much simpler process when you get some outside help. That said, it's important not to interpret the lack of specific government regulations on how to secure your IT platforms as an indication that you should do nothing. Help is available and in the long run, much more affordable than the bill a hacker will send you to get your data back, along with the long-term ramifications of a damaged reputation.

Following our four simple steps in this article is a great start but just the first step on the road to securing your data. We understand that as a provider with patients to care for, time is never on your side. Take the pressure off and let us help you. LightPoint created a guide to help: Security Risks & Healthcare: How to Protect Your Practice. Feel free to contact us anytime to chat with one of our experts.