Is Your Practice Cyber Secure?

Author: Robin Beasley, JD, Senior Market Manager
If you have questions on this topic, please contact Mallory Earley at 888-877-4498, extension 4789, or email MalloryEarley@ProAssurance.com.

With the increased use of technology in healthcare comes the growing risk of cyberattacks and cyber liability, as well as regulatory investigations, fines, and penalties. Anything created, stored, or transmitted electronically is at risk of being compromised by an innocent mistake or—worse yet—maliciously stolen by a criminal. When it comes to data breaches, not all industries are on equal ground. Some have traditionally been much bigger targets than others, and this includes healthcare.

According to an analysis of U.S. healthcare data breach statistics, “2018 saw a 157.67% year-over-year increase in the number of compromised healthcare records. 13,236,569 healthcare records were breached in 2018.” The report further notes that nearly 195 million healthcare records—equating to the records of 59.80% of the U.S. population—have been reported stolen, exposed, or disclosed since the Department of Health and Human Services’ Office for Civil Rights began publishing summaries in October 2009. Another article shows that as of mid-2019, 11 of the 13 largest data breaches affected medical or healthcare organizations.

Many people don’t believe—or understand why—medical information is valuable or at risk.

Thieves target medical records because they contain a variety of patient information: social security numbers, as well as financial, health, demographic, and family information. Criminals can use the stolen information to steal identities and apply for credit cards, store accounts, or other lines of credit. They also use the information to purchase medical equipment and pharmaceuticals for resale. Criminals also can pose as healthcare providers and fraudulently bill health insurers or the government for fictitious medical care. One cybersecurity expert estimates that a medical record can fetch hundreds or even thousands of dollars on the black market. Meanwhile, a credit card number may go for as little as a quarter, and a social security number for as little as a dime.

Big or small, all healthcare organizations are at risk.

Healthcare organizations of all sizes—from large healthcare systems to solo practices—have all been attacked, but the size of the entity does not necessarily determine the size of the breach. One need only reference the HIPAA data breach portal to verify the truth of this assertion. Data breach incidents at very large organizations have exposed anywhere from several hundred to several million patient records. Likewise, cyberattacks on solo practices—though frequently in the range of several hundred to several thousand patient records—have exposed tens of thousands of patient records with a single breach.

59.80% of the U.S. population’s healthcare records have been stolen.
Is Your Practice Cyber Secure?

Transition to EHRs, dated systems, and weak security measures pave the way for cyberattacks.

The transition to electronic health records has given criminal hackers more opportunities to steal medical records, and the biggest reason is ease of access. Healthcare is susceptible to attacks due to its valuable data and rising complexity of systems on interconnected networks. In addition, some hospitals do not have cyber teams or adequate funding for tech security. They may not fully appreciate cyber risks, given their focus on improving patient outcomes and investment in new medical equipment. Once a hacker penetrates whatever security the system does have, the exposed information is easily compromised. The operational disruptions that can occur as a result can be debilitating.

Cyberattacks on EHR systems take many forms.

In addition to outright theft of medical information, emerging cyber threats also include various forms of cyber terrorism and cyber extortion. Recent reports of ransomware attacks are particularly troublesome. Sophisticated hackers launch malicious codes (typically via entry through email) that crawl through a target’s computer system, encrypting and locking up data files, and then demand payment (ransom) in exchange for providing the decryption key. Cybersecurity experts believe healthcare providers make good targets for ransomware attacks; they do not typically have the advanced backup systems and other resilience measures in place that are typical of other types of organizations.

What can you do to help safeguard EHRs and protect patient information?

Patient trust in your practice’s ability to protect medical information is critical. To earn and maintain that trust, it is important to have safeguards in place that help prevent data breaches. When implementing or updating an EHR system, talk to your vendor about cybersecurity. Ask whether electronically stored and transmitted information is encrypted. It is also a good idea to determine if or when the vendor will provide security updates for your EHR software.

You may need to invest more resources in shoring up the walls around your electronically stored and transmitted data. Cybersecurity is a highly specialized area that requires a certain degree of expertise and experience. Your EHR vendor may be able to provide some assistance in this area, but remember their expertise is more about creation and functionality, and less about security. Depending on the size of your practice, your best option may be hiring an in-house cybersecurity expert or contracting with a cybersecurity firm specializing in healthcare to protect your practice and your patients.

There are, of course, a myriad of technical safeguards—like using a firewall, installing and maintaining anti-virus software, regularly updating software, and routine operating system maintenance—you should have in place to protect the security of electronically stored and transmitted information. But not all cybersecurity measures have to be technical in nature. In fact, much of cybersecurity follows good common sense. One particularly helpful resource in this regard is HealthIT.gov, which is the official website for The Office of the National Coordinator for Health Information Technology (a division of the Department of Health and Human Services). They publish and regularly update a document titled “Top 10 Tips for Cybersecurity in Health Care.” Some of their recommendations fall into the common sense category, and can be found in the adjacent box.

Contact the Risk Resource Department with any questions you have at 844-223-9648 or RiskAdvisor@ProAssurance.com.

TOP TIPS FOR CYBERSECURITY IN HEALTH CARE

1. Establish a Security Culture. First and foremost, create a culture of compliance and cybersecurity awareness. HealthIT.gov states, “[t]he weakest link in any computer system is the user,” and “[s]ecurity practices must be built in, not bolted on.” The importance of cybersecurity awareness and compliance must be instilled at every level, and it must become part of your practice’s culture. The level of commitment that your practice makes to patient safety should be the same level of commitment to the safety and security of patient information.

2. Maintain Good Computer Habits. Another common sense cybersecurity tip is simply maintaining good computer habits. Basic measures like logging off and not sharing passwords can prevent unauthorized access issues that lead to data breaches. Also, understanding how to identify phishing scams—where email is used to entice a user to click on a link or open an attachment that downloads malware into your computer system—is an essential skill, especially for those who interact with systems that store and transmit patients’ medical information. Additionally, adhering to safe and responsible online practices can greatly reduce exposure to threats from hackers, swindles, malware, and more. For example, be wary of suspect-looking websites and selective about what you click on.

3. Use Strong Passwords and Change Them Regularly. Speaking of passwords, encourage and promote proper password hygiene. Enforce strong user password standards. Passwords should have at least eight characters and include uppercase and lowercase letters, numerals, and special characters. It is also important to configure systems so that passwords must be reset on a regular basis.
TOP TIPS FOR CYBERSECURITY IN HEALTH CARE

4. Control Physical Access. The most common way electronically stored information is compromised is from the loss of devices through theft or accident. Flash drives, cell phones, tablets, and laptops are particularly vulnerable to theft or loss due to their portable nature. However, thieves have also ripped hard drives out of machines and stolen entire network servers from offices. For portable devices, the best practice is to not permit electronic health information to be stored on or transmitted by such devices. If it is necessary, then cybersecurity experts recommend that the data always be encrypted. As for the physical security of desktop computers, terminals, hard drives, backup tapes, and servers, you can minimize the risk of overt theft by securing machines in locked rooms, limiting the number of physical keys, restricting access in general, and limiting the ability to remove devices from secure areas.

5. Plan for the Unexpected. Finally, recognize that despite your best efforts, sooner or later something bad will happen, so be prepared for when it does. Create backups. Have emergency and recovery plans in place for quick implementation in the event of a breach. Also, have a breach notification and patient support plan ready in the event a breach. notification and patient the event of a breach. Also, have a place for quick implementation in emergency and recovery plans in when it does. Create backups. Have bad will happen, so be prepared for efforts, sooner or later something recognize that despite your best Plan for the Unexpected. remove devices from secure areas. 

The “Top 10 Tips for Cybersecurity in Health Care” and other resources—such as the Department of Homeland Security, the American Hospital Association, the Centers for Medicare & Medicaid Services, and the National Institute of Standards and Technology—are listed at the end of this article. These are just a few of the vast resources available to hospitals and facilities regarding cybersecurity. One of our ProAssurance risk advisors can also assist you with questions at 844-223-9648 or RiskAdvisor@ProAssurance.com.

ProAssurance also helps protect your practice against cyber liability threats.

One additional way to plan for the unexpected is to properly insure your practice against the inherent risks of cyber liability exposure. ProAssurance is committed to helping you reduce uncertainty and increase the control you have over cybersecurity—it’s only fair. That’s why we worked with Tokio Marine HCC (formerly NAS Insurance Services) to provide coverage for certain types of cyber liability risk exposures. This coverage, called CyberAssurance® Plus, is now embedded in many ProAssurance professional liability insurance policies at no additional cost. CyberAssurance Plus coverages include network asset protection, privacy breach response costs, patient notification, patient support, and credit monitoring expenses, privacy and security liability, and regulatory defense and penalties costs. It also provides coverage for multimedia liability, cyber extortion, cyber terrorism, payment card industry data, security standard assessments, proactive privacy breach response costs, and voluntary notification expenses. A unique benefit called BrandGuard® provides coverage for lost revenue due to an adverse media report or customer notification of a security or privacy breach.

While CyberAssurance Plus provides base incident and aggregate annual limits, policyholders may purchase higher coverage limits for cyber liability threats through ProSecure®. Underwritten by Tokio Marine HCC and designed to work seamlessly with CyberAssurance Plus, ProSecure is available in $1 million increments. To learn more about adding ProSecure or about the base limits provided by CyberAssurance Plus, contact your ProAssurance licensed agent or broker, or call ProAssurance at 800-282-6242.

ProAssurance insureds and their staff have access to the CyberNET® Data Security Risk Resource & HIPAA website through their ProAssurance.com account. CyberNET’s resources include:

- **Compliance tools**—HIPAA/HITECH regulations, privacy and data security basics, healthcare-specific guidance for federal and state privacy laws, and self-audit checklists
- **Training**—HIPAA compliance videos and courses on ransomware, social engineering and other data security topics, webinars, and training guides
- **Risk reduction tools**—Risk assessment workbooks, incident response plan instructions, vendor/third party risk management, and privacy/security best practices
- **Breach guidance**—Prevention methods and notification requirements
- **Sample policies, plans, and procedures**—Topics include email, passwords, device, hardware, third party management, information security/classification, vendors, remote access, and personal device user agreements

Please Note: Content on the CyberNET Data Security Risk Resource Website is provided by third party sources. ProAssurance is not responsible for the content and does not consider it to be legal advice. 

For more information about cyber liability, cybersecurity, CyberAssurance, or ProSecure, contact your agent, broker, or ProAssurance representative.
Endnotes


2 Ibid.


