ProAssurance
Treated Fairly

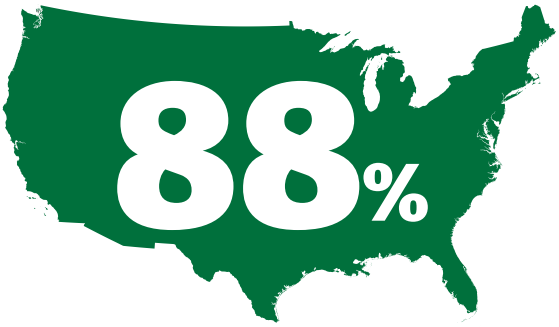
KEY considerations
For Healthcare Organizations

PROMOTING PATIENT SAFETY • PROVIDING SOUND ADVICE • PLEDGING TREATED FAIRLY

VOLUME 12 • SUMMER 2019

Is Your Healthcare Organization Cyber Secure?

Author: Robin Beasley, JD, Senior Market Manager



Of the **918** worldwide data security incidents, **808**—approximately 88%—occurred in the United States

With the increased use of technology in healthcare comes the increased 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 a recent compilation of data breach statistics, 1.9 billion data records were stolen or lost in 918 data security incidents worldwide during the first half of 2017. That's approximately 11 million data records every day, 437,815 data records every hour, 7,297 data records every minute, or 122 data records every second. Of those 918 data security incidents, 808 occurred in the United States, and 228 of them—approximately 25%—were breaches of medical or healthcare information, accounting for over 31 million compromised patient data records.[1]

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

Medical records are targeted because they contain a variety of patient information: social security numbers, financial, health, demographic, and family data. This gives criminals many potential uses for the stolen information, including identity theft and applying for credit cards, store accounts, or other lines of credit. They also use the information to purchase medical equipment and pharmaceuticals that can be resold—or to masquerade as healthcare providers to 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. In contrast, a credit card number may go for as little as a quarter, and a social security number for as little as a dime.[2]

Big or small, all healthcare organizations are at risk.

The size of the entity does not necessarily determine the size of the breach. Large healthcare systems, hospitals, facilities, surgery centers, group practices, and individual healthcare providers have all been attacked. One need only reference the HIPAA data breach "Cases Currently Under Investigation" list[3] 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 small solo practices—though frequently in the range of several hundred to several thousand—have exposed tens of thousands of patient records with a single breach.

Continued on page 2

Continued from page 1

Is Your Healthcare Organization Cyber Secure?

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

The transition to electronic health records (EHRs) has given criminal hackers more opportunities to steal medical records, and the biggest reason is ease of access. Many hospitals and healthcare facilities are using EHR systems that have not been updated in more than ten years. While hospitals and physician practices grappled with more urgent matters like ICD-10 implementation and meaningful use, robust cybersecurity measures fell down the priority list. Once a hacker penetrates whatever security the system does have, the exposed information is there for the taking.[4]

Cyberattacks on EHR systems take many forms.

In addition to outright theft of medical information, emerging cyber threats also include various forms of cyberterrorism and cyber extortion. Recent reports of ransomware attacks are particularly troublesome. Sophisticated hackers launch malicious codes (often via entry through email) that crawl through a target's computer system, encrypting and locking up data files. The hackers then demand payment (ransom) in exchange for providing the decryption key. Cybersecurity experts believe healthcare providers make good targets for ransomware attacks because they do not usually have the advanced backup systems and resilience measures other organizations typically use.[5]

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

Patient trust in your facility'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. Hiring an in-house cybersecurity team and contracting with a cybersecurity firm specializing in this area may be the best options to protect your facility and your patients.

There are, of course, a myriad of technical safeguards—using a firewall, installing and maintaining anti-virus software, routinely updating software, and operating system maintenance—that can help hospitals and facilities protect the security of electronically stored and transmitted information. However, not all cybersecurity measures are technical. In fact, good common sense also helps create a more secure environment.

One particularly useful resource in this regard is HealthIT.gov, the official website for The U.S. Department of Health and Human Services' Office of the National Coordinator for Health Information Technology. They publish and regularly update "Top 10 Tips for Cybersecurity in Health Care."[6] Some of their recommendations fall into the common sense categories as follows:

1. **Establish a Security Culture.** First and foremost, create a culture of compliance and cybersecurity awareness. In their words, "[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 organization's culture—the safety and security of patient information is as critical to your organization as its commitment to patient safety.
2. **Maintain Good Computer Habits.** Simple 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 is essential for all computer users, especially those who interact with systems that store and transmit patients' medical information. By adhering to safe and responsible online practices—like being continually wary of suspect-looking websites and selective about what you click on—you can greatly reduce exposure to threats from hackers, scams, and malware.
3. **Use Strong Passwords and Change Them Regularly.** 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 passwords must be reset regularly.
4. **Control Physical Access.** The most common way electronically stored information is compromised is by accidental loss or theft of devices. Flash drives, cell phones, tablets, and laptops are particularly vulnerable due to their portable nature. The best practice is to prohibit storage or transmission of electronic health information by such devices. If that is not feasible, cybersecurity experts recommend that the data always be encrypted. More substantial devices are also at risk: hard drives have been ripped out of machines and entire network servers have been stolen from facilities. To help protect your desktop computers, terminals, hard drives, back-up tapes, and servers from overt theft:
    - Keep machines in locked rooms
    - Limit the number of physical keys
    - Restrict access in general
    - Further restrict the ability to remove devices from secure areas

Continued on page 3

Continued from page 2

Is Your Healthcare Organization Cyber Secure?

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 plans and recovery plans ready for quick implementation if a breach occurs. In addition, keep breach notification and patient support plans current in case you are required to notify those whose records were exposed.[7]

There are many government and industry sources for healthcare cybersecurity information. Visit the websites of The Department of Homeland Security, American Hospital Association, National Institute of Standards and Technology, and Centers for Medicare & Medicaid Services for resources available when this article was published.[8]

The transition to electronic health records (EHRs) has given criminal hackers more opportunities to steal medical records, and the biggest reason is ease of access.

ProAssurance also helps protect your healthcare organization against cyber liability threats.

One additional way to plan for the unexpected is to insure your hospital or facility against the inherent risks of cyber liability exposure. ProAssurance is committed to helping you reduce uncertainty and help increase the control you have over cyber threats. That's why we partnered with NAS Insurance Services (NAS) to provide coverage for certain types of cyber liability risk exposures. This coverage, called CyberAssurance® Plus, is embedded in many ProAssurance healthcare professional liability insurance policies for hospitals and facilities at no additional cost. CyberAssurance Plus coverage includes network asset protection, privacy breach response costs, patient notification expenses, patient support and credit monitoring expenses, and 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, voluntary notification expenses. A unique coverage feature called BrandGuard® provides coverage for lost revenue as a result of 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 NAS 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**.

More Cyber Risk Resources for ProAssurance Insureds through NAS Insurance Services (NAS)

ProAssurance-insured hospitals and facilities and their staff also have access to webinars, tool kits, bulletins, posters, FAQs, and online training programs to help address cyber liability risks. For example, you can access:

- Summaries of major changes to the HIPAA/HITECH Rules (which became effective September 2013), including required changes to your Notice of Privacy Practices; the expanded definition of Business Associates (with updated sample Business Associate and Vendor Agreements); and patients' ability to request medical records in electronic form
- Webinars, tool kits, and sample documents, including basic data privacy/security, encryption, and destruction practices; sample HIPAA Privacy/Security Rule policies and procedures; social media training tools; sample mobile and personal device user policies, procedures, and agreements; and how to implement a data security plan
- Breach notification requirements under federal and state laws (where applicable); sample HIPAA Breach/Risk Assessment Worksheets; examples of incidents to report, how to report data security incidents, and much more

ProAssurance insureds can access these resources from NAS' Data Security Risk Management website through their ProAssurance.com accounts.

Please Note: Content on the NAS 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 risk management or other healthcare risk resource issues, insureds may contact the ProAssurance Risk Resource team at **844.223.9648** or **RiskAdvisor@ProAssurance.com.**

Continued on page 4

ProAssurance
Treated Fairly
Professional Liability Insurance & Risk Resource Services

KEY considerations
For Healthcare Organizations

2600 PROFESSIONALS DRIVE, OKEMOS, MI 48864

PRSRT STD
US POSTAGE
PAID
PROASSURANCE
48924

Continued from page 3

Endnotes

1 "First Half 2017 Breach Level Index Report: Poor Internal Security Practices Take a Toll," September 20, 2017, https://www.gemalto.com/press/pages/first-half-2017-breach-level-index-report-identity-theft-and-poor-internal-security-practices-take-a-toll.aspx, accessed May 22, 2018.

2 Mariya Yao, "Your Electronic Medical Records Could Be Worth $1000 To Hackers," Forbes, April 14, 2017, https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#c2b077350cf1, accessed May 22, 2018.

3 "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, accessed May 18, 2018.

4 Carolyn Johnson, Matt Zapotosky, "Under pressure to digitize everything, hospitals are hackers' biggest new targets." The Washington Post, April 1, 2016, https://www.washingtonpost.com/news/wonk/wp/2016/04/01/under-pressure-to-digitize-everything-hospitals-are-hackers-biggest-new-target/?utm_term=.9ed3a0ec1464, accessed May 22, 2018.

5 Joseph Conn, "Hospital pays hackers $17,000 to unlock EHRs frozen in 'ransomware' attack," Modern Healthcare, February 18, 2016, http://www.modernhealthcare.com/article/20160217/NEWS/160219920 accessed May 22, 2018.

6 "Top 10 Tips for Cybersecurity in Health Care," HealthIT.gov, https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf, accessed May 22, 2018.

7 Ibid.

8 "Cybersecurity," Department of Homeland Security, http://www.dhs.gov/topic/cybersecurity, "Cybersecurity," American Hospital Association, http://www.aha.org/advocacy/leveraging-technology/cybersecurity, "Cybersecurity Framework," National Institute of Standards and Technology, http://www.nist.gov/cyberframework, and "Homeland Security Threats," Centers for Medicare & Medicaid Services, https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Homeland-Security-Threats.html, all accessed May 22, 2018.

If you have questions or a change of address, please call 800.282.6242.

Key Considerations is published twice annually by ProAssurance's Risk Resource Department
Phone: **844.223.9648** • Email: **RiskAdvisor@ProAssurance.com**

Mallory Earley, JD, Senior Risk Resource Advisor

Policyholders may find Risk Resource articles and information archived on our website: ProAssurance.com/Newsletters.

ProAssurance
Treated Fairly
SINCE 2007 WARD'S 50

ProAssurance Group is rated **A+ (Superior)** by A.M. Best.

ProAssurance Indemnity Company, Inc., ProAssurance Casualty Company, and ProAssurance Specialty Insurance Company, Inc. are subsidiaries of ProAssurance Corporation.