Cybersecurity and healthcare records

Tips for ensuring patient safety and privacy.

By Susan Conaty-Buck, DNP, APRN, FNP-C

Rachel is a nurse working on a hospital unit charting notes in the electronic health record (EHR). She suddenly remembers that it's her best friend's birthday and she's forgotten to get her a gift. When Rachel completes her patients' notes, she opens a browser on the hospital's computer to see if she can find something online for her friend, although personal use is prohibited. She opens several sites until she finds the right gift. She doesn't recognize the name of the site but it promises quick delivery, so she places the order and pays with a credit card.

Later in the day, the hospital's EHR starts to operate slowly and introduces errors. That night, a message appears on all of the hospital's computer monitors: "You've been hacked. All data encrypted. Bitcoin message later. Pay or records sold." The hospital's information technology (IT) team races to limit the damage. The system is shut down for days, elective procedures are cancelled, records have to be obtained from backup sources, and staff performs downtime charting. The hospital was the victim of a cybercrime using ransomware because Rachel opened the door to an intruder.

How cybercrime happens

Despite increased precautions, cybercrime continues to rise. (Visit americannursetoday.com/cybersecurity-and-healthcare-records to find out what the U.S. government is doing to fight it.) In 2016, more than 16 million patient records were stolen from healthcare organizations in the United States, and more than 150 million individuals have had their medical records stolen since 2010. Most thefts were the result of attacks against EHRs, and in many cases, a simple employee error opened the door to the attack. (See *Cybercrime lingo*.)

Other points of access for cybercrooks include stolen laptops with inadequate data protection, infected USB flash drives plugged into a healthcare system computer, and wireless networks used by many personal devices, such as smart phones, tablets, and laptops. In addition, the increasing demands of the workplace mean that sometimes healthcare providers may bypass appropriate data protection. Transmitting private healthcare data without secure protocols, encryption, and strong passwords puts the healthcare organization's financial, administrative, and clinical information systems at risk for attack and ultimately patient harm.

Cybercrime lingo

Many cyberattacks begin when someone clicks on what appears to be an innocent link. This click can lead to a:

- ***virus*** that infects software and reproduces copies of itself when the software is opened.
- ***worm*** that infects software and spreads copies without the user taking action.
- ***Trojan*** that appears to be safe software but contains malware that acts when downloaded and opened.

Here are some other ways cybercriminals can cause trouble:

- ***Ransomware*** is malware that keeps users from accessing their system or device or encrypts files until a fee (ransom) has been paid.
- ***Rootkits*** hide malware from antivirus detection and removal programs.
- ***Keystroke*** logger programs record user keystrokes to help cyberthieves acquire passwords.
- ***Adware*** produces a script or code that automatically downloads malware. Sometimes a user is offered a malware removal tool for fake malware, but it's really a ploy to install a Trojan or ransomware.

The price of healthcare data theft

The average price paid on the black market for stolen healthcare information as part of a full identity profile ranges from $20 to $50. Stolen medical records are more profitable than simple financial data because of its potential com-

plexity. Healthcare data has a long life—a person can change banks and credit cards but not past medical history. With access to healthcare data as well as financial and credit card data, cybercriminals get both short- and long-term benefits. Evidence shows that stolen healthcare records are often sold and resold on the dark web.

Healthcare organizations (and ultimately patients) pay heavy prices for data breaches. The organization may have to pay civil penalties to the U.S. Department of Health and Human Services' Office for Civil Rights (ORC), which enforces Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. Breaches of unsecured health information that affect 500 or more individuals must be publicly reported on the ORC website. And each state has provisions related to HIPAA rules and may impose additional penalties. The U.S. Department of Justice also may enforce criminal penalties for HIPAA violations. Penalties for noncompliance are based on the level of negligence, and federal fines can range from $100 to $50,000 per violation, with penalties of $1.5 million to $5.5 million. The Federal Trade Commission may levy fines of $16,000 per violation. Class action lawsuits of $1,000 per record and 2 or more years of ongoing credit monitoring for patients paid for by the healthcare agency are common. A recent report shows that the average cost per record for a healthcare breach is $380. (See *The cost of security breaches*.)

Compounding the loss of data and financial penalties is patient defection to other practices. According to Security Metrics, up to 40% of patients whose healthcare information has been involved in a breach will leave the affected practice. The loss of patient trust is significant. A 2016 Pew Research report found that roughly 50% of Americans don't trust the federal government or social media to protect their data. Despite this, 64% of Americans have online accounts that involve health, financial, or other sensitive data. Of these, 32% have online accounts with their healthcare providers, and increasing numbers have been encouraged to communicate via patient portals. The cost of paying for increased technology, cybersecurity staff, and potential fines drives up healthcare premiums for all consumers.

The cost of security breaches

When electronic health record security is breached, hospitals and other organizations often pay hefty fines. Here are a few examples.

Advocate Health Care
Fine: $5.55 million
Why: Four stolen laptops with data from 4 million patients.

Alaska Department of Health and Social Services
Fine: $1.7 million
Why: Stolen USB drive containing personal health information, and lack of adequate policies and procedures to safeguard electronic health information.

Anthem in Indiana
Fine: $115 million
Why: Breach affected nearly 80 million patients when a hacker accessed a database including names, birthdays, social security numbers, addresses, email addresses, and employment and income information.

New York–Presbyterian Hospital and Columbia University
Fine: $4.8 million.
Why: Physician attempted to deactivate a personal computer, leaving data unsecured.

Oregon Health & Science University
Fine: $2.7 million
Why: Data breaches affecting 7,000 patients as the result of a stolen laptop and data stored in an unapproved Google Cloud.

Individual and organizational steps

Steps to preventing cyberattacks of EHRs include healthcare worker education, which should begin in school, password security, data encryption, and patient education.

Healthcare worker education

All healthcare employees should learn about cybersecurity risks and work to protect patient privacy and safety. The U.S. Department of Homeland Security offers tips in its *Stop.Think.Connect* national campaign (dhs.gov/stopthinkconnect), encouraging all Americans to improve online safety.

Healthcare organizations should provide mandatory cybersecurity competency programs. The education and training can be fun, using online privacy and security games, such as those offered by HealthIT.gov (healthit.gov/providers-professionals/privacy-security-training-games), or challenges that include sending staff random phishing messages to increase their recognition of potential cyberattacks. To ensure threats are contained quickly, policies for reporting accidental breaches should emphasize that staff will not be penalized.

Password security

Steps to ensuring password security include changing it frequently, storing it in a safe place, and not sharing it with others. A Verizon Enterprise 2016 Data Breach Investigations report found that "63% of confirmed data breaches involved leveraging weak, stolen, or default passwords." To help develop secure passwords and remember them, organizations and individuals can use a password generator and a password safe.

Many organizations require multi-

factor authorization, which can include a PIN number or a biometric measure using fingerprint or facial-recognition software.

Data encryption

Data encryption is required for all electronic devices used to record, store, and transmit patient data so if equipment is lost or stolen, the data can't be downloaded. Healthcare organizations should have a mobile device compliance policy. Some organizations provide employees with mobile devices with installed security, while others allow employees to use their own technology but require use of specific security applications in the workplace. Any mobile device used for secure patient data should be routinely scanned to ensure that it has the most up-to-date security software.

Any technology used for patient care—including personal devices—must be equipped with remote wipe technology that allows the user to remotely erase all data from a lost or stolen device. Additional tips for securing mobile devices are available at https://goo.gl/zG1mjT.

Patient education

Nurses and other healthcare workers can teach patients about the safe use of personal health information technologies. Helping patients understand the risks of unsecure communication and the need to communicate only though encrypted patient portals is a responsibility of all healthcare personnel. Nurses also can encourage patients to read personal health information technology agreements to understand the use and ownership of their personal data by third parties.

Remind patients with implanted or connected medical devices to keep alert for messages sent from the manufacturer about product updates and revisions, and to seek immediate help if the device doesn't appear to be working correctly. (See *Medical device security*.)

Cybersecurity is everyone's business

Many patients receive care from a number of clinicians and staff working in teams or as individuals. Everyone on the team, no matter his or her role, must actively ensure patient safety and privacy. It takes only one click to let a cyberthief in the door—think before you click.

So, what happened to Rachel? The hospital's cybercrime team traced the breach back to her use of the system, noting that she accessed more than 10 sites with irregular webpages and email addresses. Because hospital policy prohibited personal use of the hospital's computers, the system was not configured to warn users about potentially dangerous email addresses. Even if Rachel had been warned and realized that she enabled the cyber breach, the hospital had no forgiveness plan for potential offenders. Because Rachel had violated computer use regulations and her actions caused injury to the hospital, staff, and potentially to patients, she was fired. ★

To learn what you can do about cybersecurity in your organization, turn to page 65.

Medical device security

Many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity attacks. If these devices are hacked, an unauthorized user could remotely alter the transmitter of a patient's radio frequency–enabled device and cause harm. In 2017, St. Jude's implantable cardioverter defibrillators and cardiac resynchronization therapy defibrillators underwent multiple software updates to prevent external manipulation and potential patient injury. Many medical devices that connect to an electronic network, such as medication pumps, surgical robotics, and deep brain stimulators, carry similar risks, and manufacturers are working to make them less vulnerable to being hacked.

Susan Conaty-Buck is is a an assistant professor of nursing, a family nurse practitioner, and a researcher in health information technology at the University of Delaware in Newark.

Selected references

Arora S, Yttri J, Nilsen W. Privacy and security in mobile health (mHealth) research. ARCR: Alcohol Research: *Current Reviews*. 2014;36(1):143-51.

Cerrato P. How well protected is your protected health information? Perception versus reality. In: *Protecting patient information: A decision-maker's guide to risk, prevention, and damage control*. Cambridge, MA: Syngress; 2016: 3-18.

Coronado AJ, Wong TL. Healthcare cybersecurity risk management: Keys to an effective plan. *Biomed Instrum Technol*. 2014;48(1): 26-30.

FDA issues reminder on cybersecurity for networked medical devices. *Biomed Instrum Technol*. 2010;suppl 4.

Fu K, Blum J. Controlling for cybersecurity risks of medical device software. *Biomed Instrum Technol*. 2014;48(1):38-41.

Imgraben J, Engelbrecht A, Choo K-KR. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behav Inf Technol*. 2014;33(12):1347-60.

Kim L. Cybersecurity awareness: Protecting data and patients. *Nursing*. 2017;47(6):65-7.

Krisberg K. Cybersecurity: Public health increasingly facing threats. *Am J Public Health*. 2017;107(8):1195.

McCallister S. Totally avoidable causes of data breaches. July 21, 2016. physicianspractice.com/technology-survey/totally-avoidable-causes-data-breaches

Middaugh DJ. (2016). Do security flaws put your patients' health at risk? *Medsurg Nurs*. 2016;25(2):131-2.

National Conference of State Legislatures. Security brief notification laws. April 12, 2017. ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Olmstead K, Smith A. Americans and cybersecurity. 2017. pewinternet.org/2017/01/26/americans-and-cybersecurity

Perakslis ED. Cybersecurity in health care. *N Engl J Med*. 2014;371(5):395-7.

Ponemon Institute LLC. The aftermath of a data breach: Consumer sentiment. April 2014. ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf

Proctor RW, Chen J. The role of human factors/ergonomics in the science of security: Decision making and action selection in cyberspace. *Hum Factors*. 2015;57(5):721-7.

Rios B. Cybersecurity expert: Medical devices have 'a long way to go.' *Biomed Instrum Technol*. 2015;49(3):197-200.

What can I do about cybersecurity?

It's every employee's responsibility to protect the organization, other employees, and patients from cyber attack. Here are some suggestions to help you fulfill that responsibility.

Choose a secure password. Use passwords that are at least eight characters long and a mix of letters, numbers, and characters. Don't include personal information such as your pets' names. Consider using phonetic replacements such as "PH" for "F."

Keep your password secure. Don't share usernames or passwords with anyone. Use different passwords for different accounts so someone who finds one password can't access multiple accounts.

Delete emails, messages, and attachments from unknown sources. Never open an attachment from a source you don't know. And don't click on any embedded links; cybercriminals sometimes use these attachments to access systems.

Use data encryption for all devices. If your organization allows you to use your own device for work, ask what security you need to set up.

Download updates. Be sure you have the most up-to-date operating system and security software.

Educate others. Be sure colleagues and patients understand the need for cybersecurity. Consider extending your reach beyond the healthcare setting by using targeted materials for different groups available from the Stop. Think. Connect. Campaign. (dhs.gov/stopthinkconnect-toolkit).

Report any concerns. If you experience any unusual problems with a device or receive a suspicious electronic message, notify your information technology (IT) department.

Access resources from the Stop. Think. Connect. This Department of Homeland Security campaign is intended to increase understanding of cyberthreats and empower people to be safer and more secure online. Access the website (dhs.gov/stopthinkconnect) to download resources, including posters, brochures, videos, and tip cards. You can become a friend of the campaign at dhs.gov/friends-campaign-program and explore various resources at stcguide.com.

Cybersecurity resources for individuals and organizations

Depending on your practice setting, you or your organization may find these resources helpful.

Cybersecurity information available from the U.S. Government.

- National Cyber Awareness System Products. Information useful for overall awareness. (us-cert.gov/ncas).
- U.S. Department of Health and Human Services. Information security and privacy program. (hhs.gov/ocio/securityprivacy/index.html)
- U. S. Food & Drug Administration (FDA). Fact sheet: The FDA's role in medical device cybersecurity. (fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf).

Cybersecurity tools

- **Guide to privacy and security of electronic health information** (healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf)—includes a sample seven-step approach for implementing a security management process.
- **Security risk assessment (SRA) tool** (healthit.gov/providers-professionals/security-risk-assessment-tool)—tool to help navigate the security risk analysis process.
- **Certified Health IT Product List** (chpl.healthit.gov/#/search)—Office of the National Coordinator for Health Information Technology (ONC's) listing of electronic health records (EHRs) and EHR modules that have been tested and certified under the ONC Health IT Certification Program.