CYBERSECURITY FOR OPHTHALMOLOGISTS

How to protect your practice.

BY RENEE C. BOVELLE, MD, MCS

Today's health care system is inextricably linked to cyberspace by our quest to provide innovative and effective outcomes to patients. We use internet-connected diagnostic equipment, telemedicine, AI, and data digitization every day for research, revenue cycle management, and improving and preserving vision. Patients trust us to use these technologies wisely and safely, so we must understand best practices for securing patient data.

The explosion of ransomware and other cyberattacks is an unwelcome challenge. Health care data breaches reached an all-time high during the COVID-19 pandemic and affected 45 million people in 2021. The US Department of Health and Human Services documented a significant rise in hacking incidents at outpatient/specialty clinics in 2021—an increase of 41% compared to 2020.[1]

WHY HEALTH CARE IS A TARGET

Health records are a rich source of valuable personal information for criminals. They hold an array of sensitive and protected patient data, including demographic and insurance information; employment, financial, and medical history; email address; Social Security number; and the contact information for relatives and close personal associates.

Ambulatory surgery centers and small to medium outpatient facilities are especially vulnerable to cyberattacks because of the increased staff turnover associated with the pandemic. Such facilities also have fewer resources to devote to cybersecurity than larger entities.

When protected health information (PHI) is breached, patients may need to cancel their credit cards, although they can dispute charges and bogus transactions are often traceable. In contrast, PHI generally cannot be changed, discarded, or reissued. Like a fingerprint, PHI is connected to an individual forever. Medical records can be worth up to $1,000 depending on completeness.[2]

CRIMINAL USAGE OF PHI

Stolen medical identities can be used for various purposes, including insurance fraud, identity theft, and other means of financial gain. Many news stories feature victims whose medical information has been used for prescription fraud or to obtain medical care. Such theft can have national security implications.

Anthem and Premera Blue Cross were hacked in 2014 and 2015, which coincides with the federal government's breach at the US Office of Personnel Management.[3] Officials in the intelligence community attributed all three attacks to actors in China. An adversary may attempt to compromise government employees whose information has been breached and first identify them by cross-checking data from multiple breaches.[4]

CONSEQUENCES OF A DATA BREACH

For patients. Our prime objective is to promote, maintain, and restore health. Data breaches may interfere with achieving these goals. Researchers at Vanderbilt University examined the 30-day mortality rate of patients with acute myocardial infarction after data breaches between 2011 and 2015. They found that hospital data breaches were associated with a statistically significant increase in the 30-day mortality rate. Moreover, they estimated that health care data breaches were linked to more than 2,000 deaths per year in the United States.[5]

These findings suggest a correlation between mortality and data breaches and indicate that the health care industry should invest in cybersecurity education for physicians to improve patient privacy and outcomes. Data breaches can also prevent us from accessing previous medical records and interfere with our research.

The Medical Identity Fraud Alliance is an alliance of health plans, providers, consumer organizations, industry, and other health care stakeholders that seeks to prevent medical identity fraud. The Medical Identity Fraud Alliance sponsored the Ponemon Institute's Fifth Annual Study on Medical Identity Theft, which found that medical identity fraud has substantial fiscal repercussions for the injured party. In a survey for the study, 65% of respondents paid an average of $13,500 to deal with the aftermath

of medical identity fraud. The study's conclusions included the following:

- Medical identity theft is financially costly to patients;
- Medical identity theft can adversely affect patient reputations; and
- Patients expect health care providers to be proactive in preventing and detecting identity theft.[6]

For physicians. HIPAA, the Health Information Technology for Economic and Clinical Health Act, and corresponding state laws require us to employ "reasonable" cybersecurity measures to protect patients' PHI. Failure to apply the most currently accepted reasonable measures can result in stiff fines and repercussions such as loss of reputation and revenue. The requirements are nonnegotiable and make no distinction between a physician who is cognizant of the cybersecurity mandates and one who is not.

Beyond the penalties, ransomware can force a small office to close.[7]

HOW TO REDUCE THE RISK OF A DATA BREACH

We must take a leadership role in promoting cyber hygiene at our practices. It is also important to have a cybersecurity expert educate staff. Several other steps can help protect practices against a data breach.

Create a culture of cybersecurity awareness. Passwords should not be shared. Patient data should not be emailed without encryption. Everyone at the practice should be educated on how to identify suspicious emails. Annual and new-hire training on proper cybersecurity protocols should be established.

Employ technology to assist with cybersecurity. This technology includes firewalls, Wi-Fi and email security, and endpoint protection. Allowing staff to open personal emails on the business network may increase risk.

Choose secure business associates and vendors. It is essential to have a business associate agreement with each vendor that has access to patient data. A business associate agreement between the health care organization and the associate must contain written assurances that the associate will protect against the disclosure of PHI.

Control access to patient data. Practices should allow access to PHI based on necessity. Not all staff members and business associates need access to all patient data. Multifactor authentication can also be used, especially on public-facing portals or for remote workers.

Employ both information technology and cybersecurity professionals. Just as a comprehensive ophthalmologist differs from a retina specialist or neuroophthalmologist, information technology (IT) and cybersecurity are separate roles. We all have a list of specialists we refer to when needed. Likewise, we should have a cybersecurity professional to refer to when needed rather than wait until we have an emergency to find one.

Update software. It is imprudent to use legacy systems or software that is outdated and no longer supported with patches. For example, Windows XP and Windows 7 (Microsoft) are no longer supported. Diagnostic equipment using this software may still work, but the operating system is vulnerable to attack. Work with your IT professional to ensure your system is resilient and up to date, including patching vulnerabilities.

Create a cybersecurity policy and procedures manual. Work with IT and cybersecurity professionals to create a cybersecurity policy and procedures manual. It should account for remote work, personal device use, and current data privacy considerations for employee access to documents and other information.

Obtain cyber liability insurance. Having third-party cyber insurance can help ensure that a practice has proper protection. It can also help mitigate revenue loss, business disruption, equipment damage, legal fees, public relations expenses, and forensic analysis if a data breach occurs.

WHAT TO DO AFTER A DATA BREACH

Practices should develop an incident response plan that outlines the procedures and steps to be followed after a cyberattack and employ the plan if a cyberattack occurs. The incident response plan should document the roles and responsibilities of each individual at the practice for detecting, responding to, and limiting the consequences of a data breach. Immediate steps may include the following:

- Notify the practice's cybersecurity professional;
- Disconnect the network from the internet if possible;
- Disable remote access;
- Maintain firewall settings;
- Install pending security updates or patches;
- Change passwords; and
- Notify the practice's cyber insurance company.

Having an incident response plan to reference following a cyberattack can help the organization restore the compromised networks and recover from the damage quickly.

Similar to an ophthalmic emergency, it is crucial to recognize the condition early, prepare a plan in advance, and have tools available to mitigate damage. ■

1. Landi H. Health care data breaches hit all-time high in 2021, impacting 45M people. *Fierce Healthcare*. February 1, 2022. Accessed May 12, 2022. https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people
2. Jercich K. Tens of thousands of patient records posted to dark web. *Healthcare IT News*. February 10, 2021. Accessed May 12, 2022. https://www.healthcareitnews.com/news/tens-thousands-patient-records-posted-dark-web
3. $16 million Anthem HIPAA breach settlement takes OCR HIPAA penalties past $100 million mark. *HIPAA Journal*. October 16, 2018. Accessed May 12, 2022. https://www.hipaajournal.com/16-million-anthem-hipaa-breach-settlement-takes-ocr-hipaa-penalties-past-100-million-mark
4. Bennett B, Hennigan WJ. China and Russia are using hacked data to target U.S. spies, officials say. *Los Angeles Times*. August 31, 2015. Accessed May 12, 2022. https://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html
5. Choi S, Johnson EM. Do hospital data breaches reduce patient care quality? arXiv: *General Economics*. April 3, 2018. Accessed May 12, 2022. https://arxiv.org/pdf/1904.02058.pdf
6. Fifth Annual Study on Medical Identity Theft. Ponemen Institute. February 2015. Accessed May 12, 2022. http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf
7. Lehmann C. Docs refused to pay the cyber attack ransom - and suffered. *Medscape*. January 13, 2022. Accessed May 12, 2022. https://www.medscape.com/viewarticle/966051

RENEE C. BOVELLE, MD, MCS
■ Howard University Department of Ophthalmology, Washington, DC
■ rcbeye@gmail.com
■ Financial disclosure: None