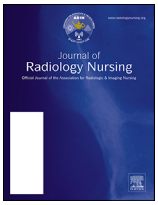
Journal of Radiology Nursing 38 (2019) 13–14

Contents lists available at ScienceDirect

Journal of Radiology Nursing

journal homepage: www.sciencedirect.com/journal/journal-of-radiology-nursing



Legal Awareness

Cybersecurity: Why Should We be Concerned?

Shawna M. Butler, DNP, JD, RN, CPHRM *

Massachusetts General Hospital, Boston
University of Massachusetts, Boston

Although many will laud the benefits of technology in health care, there are some risks associated with its increased use within the industry. Not only institutions but also individual clinicians should be concerned about this growing threat. Cybersecurity is now everybody's concern. Hacking and information technology security incidents have been on the rise in the past few years as the adoption of electronic health records has expanded (Bai, Jiang & Flasher, 2017).

Why hack health records?

Hackers choose their targets as crimes of opportunity. They focus on 2 specifics: (1) does the target have the personal identifying information? and (2) can it infiltrate the network? (ASHRM, 2018). Some may wonder what they will gain by hacking these institutions. There are unfortunately many ways they can benefit maliciously. They may sell the information on the dark Web, sell health insurance information to the uninsured, sell information to organizational competitors, use sensitive health information to extort payments, or extort payment to release locked or encrypted files (ASHRM, 2018).

What is the Health Insurance Portability and Accountability Act privacy rule?

The targeted information is regulated via the Health Insurance Portability and Accountability Act (HIPAA). The privacy rule under HIPAA includes all medical records and individually identifiable health information. This information is referred to as protected health information (PHI). PHI includes name, address, birth date, and social security number (not an exclusive list). Some may deem this information even more valuable than credit cards, bank accounts, and so forth. (ASHRM, 2018).

What exactly is a breach?

A breach is the impermissible use or disclosure of unsecured PHI which compromises the security or privacy of the protected information. Once a breach of unsecured PHI is identified, covered entities (health-care providers, health plans, and so forth) are required to notify both the involved individuals and the Secretary of Health and Human Services. In some circumstances, they may also be required to notify the media as well. There is also legislation in all 50 states requiring private or governmental entities to notify individuals of security breaches (in addition to the federal requirement via HIPAA) (ASHRM, 2018).

In addition to having to notify affected individuals, there are other costs of data breaches. In addition to fines, there may be other financial costs associated with services, such as remediation expenses, legal fees, business interruption, and restoration of network. Reputational damage may also have far more implications than solely financial (ASHRM, 2018).

How are cybercriminals so successful?

Cybercriminals use social engineering to infiltrate systems. Social engineering manipulates people to give up confidential information such as passwords or private information. This can be performed by insiders (ie, employees) providing information innocently not realizing it is a scam. The hackers may also access the employees' computers, allowing them access to the information systems by secretly installing malware. An example of social engineering that allows hackers to access systems is phishing. Mostly, everybody has received phishing emails at some point. Phishing emails may look legitimate and seem like they come from a source you may trust (ie, your boss, your bank, and so forth). The goal is to get the user to hit the malicious link. An alarming amount of cyberattacks start with a phishing email; it is reported to be as high as 91% (ASHRM, 2018). Unknowingly and without any malice, the employee is the organization's biggest vulnerability to hacks (HIPAA Journal, 2018). Therefore, all clinicians can play a part in prevention.

Statistics about breaches

Studies have shown that larger hospitals are more likely to experience a data breach, and more than one-third of hospitals where data breaches have occurred are classified as major teaching hospitals (Snell, 2017). During one study between a period in 2009 through 2016, hospitals reported 1,798 breaches of more than 500 patient records (Bai, Jiang & Flasher, 2017). There were 257 breaches reported by 216 hospitals. More than 30 hospitals

Conflict of interest: Author discloses no conflicts of interest.

* Corresponding author. University of Massachusetts, Massachusetts General Hospital, Boston 02127.

E-mail address: smbutler@partners.org.

https://doi.org/10.1016/j.jradnu.2018.12.006
1546-0843/$36.00/

experienced more than one data breach during that time frame. Four hospitals experienced three data breaches, and two hospitals experienced as many as four data breaches (HIPAA Journal, 2017). Some reports state that 2017 had the highest rate of data breach incidents yet.

Why does this occur at larger institutions?

Why larger hospitals and teaching hospitals experience more data breaches is likely due to having broader access to sensitive patient data. Although the availability of and access to patient information is ideal for providing quality health care and is considered a positive aspect in terms of patient care, it does increase risks to cybersecurity. The more the individuals who require access to data, the greater the risk of data breaches (HIPAA Journal, 2017). According to Bai, Jiang, and Flasher (2017), “a fundamental trade-off exists between data security and data access.”

What is cyber-insurance?

Cyber-insurance can be purchased to protect against breaches. Cyber-insurance may be a part of a malpractice or general business liability coverage, so it is important to verify this first. The cost of cyber-insurance coverage will vary depending on the size of practice, facility, and risk level. Some policies are ambiguous, so organizations need to do their due diligence in checking what they need to protect themselves should a breach occur (Davis, 2018).

What else can be done?

Before breaches, the senior leadership should assure that data-protection policies exist and that employees are properly trained on how to mitigate these risks. A response plan must also be available for implementation when a breach does occur. Once there is a breach, there must be a coordinated effort protocol for how to manage it and necessary notifications internally (the Board, leadership, patients, and so forth) and externally (Health and Human Services if needed) (ASHRM, 2018).

How to protect yourself and the institution as a clinician?

- Never share passwords.
- Do not send private information over unencrypted mechanisms.
- Never disable antivirus programs.
- Do not download documents or files without the permission from a supervisor, information technology, or per policy.
- Do not open unexpected email attachments.
- If you think you may have been a victim of hacking, notify the appropriate staff immediately (ASHRM, 2018).

It is everybody's responsibility to safeguard against vulnerabilities.

References

American Society of Healthcare Risk Management [ASHRM]. (Producer). (2018) Cybersecurity: Protecting your organization from the dreaded breach [video webinar]. Retrieved from http://learning.ashrm.org/. Accessed April 12, 2018.

Bai, G., Jiang, J., & Flasher, R. (2017). Hospital risk of data breaches. *JAMA Internal Med, 177*(6), 878-880.

Davis, J. (2018) *Cyber Insurance Series Part 1: What You Need to Know*. Retrieved from https://www.healthcareitnews.com/news/cyber-insurance-series-part-1-what-you-need-know. Accessed April 12, 2018.

HIPAA Journal. (2017) *Large Hospitals and Teaching-Focused Hospitals Face Greater Risk of Data Breaches*. Retrieved from https://www.hipaajournal.com/large-hospitals-teaching-focused-hospitals-greater-risk-of-data-breaches-8754/. Accessed April 12, 2018.

HIPAA Journal. (2018) *53% of Healthcare Data Breaches Due to Insiders and Negligence*. Retrieved from https://www.hipaajournal.com/53-of-healthcare-data-breaches-due-to-insiders-and-negligence/. Accessed April 12, 2018.

Snell, E. (2017) *Healthcare Breach Risk Higher in Larger Facilities. Health IT Security*. Retrieved from https://healthitsecurity.com/news/healthcare-data-breach-risk-higher-in-larger-facilities. Accessed April 12, 2018.