Cybersecurity 101: What You Need to Know

The AMA's research[i] on cybersecurity indicates that physicians are increasingly recognizing the importance of good cyber hygiene in their practices.

The increased industry focus on digital health technology, including telehealth, underscores the need for practices to consider how they will keep their patients' protected health information (PHI) private and secure. Generally, once outside data is incorporated into the patient's electronic medical record, it becomes PHI. Physicians are responsible for the privacy and security of PHI under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

WHAT YOU NEED TO KNOW ABOUT CYBERSECURITY ATTACKS:

- Cybersecurity is not just a technical issue; it's a patient safety issue.
- 4 out of 5 physicians[ii] have experienced some form of cyberattack.
- While inappropriate employee use and disclosure of PHI (e.g., inappropriate sharing or selling of patient information) are more of a concern among large health systems, phishing and viruses are the most common types of cyberattacks in small practices.

WHAT YOU NEED TO KNOW ABOUT HOW CYBERSECURITY CAN AFFECT YOUR PRACTICE/ORGANIZATION:

- Cyberattacks can cause interruptions in practice operations, compromised electronic health records (EHR) security, and direct threats to patient well-being.
- 2 out of 3 physicians have experienced downtime of up to four hours because of a cyberattack; 1 in 10 have experienced downtime of up to two days.

WHAT YOU NEED TO THINK ABOUT WHEN IMPLEMENTING TECHNOLOGY:

- Your practice's health information technology (health IT) network[iii] is comprised of several different components, and it is important to consider all of them when figuring out how to securely implement new technology. For example, not only are your practice's internet connection and EHR part of your network but also things like copiers, telephones, and practice management systems. You must also consider how a new telehealth solution will impact your health IT network, especially if outside your current EHR vendor. Physicians need to look at their networks holistically to ensure that all the "entry" and "exit" points for information coming in and out of the practice are effectively protected.
- Only 20% of small practices have internal security officers, so they typically rely on health IT vendors for security support. Physicians should understand basics about cybersecurity[iv] so that they are well informed enough to ask vendors the right questions. Such knowledge will help to equip physicians with the autonomy they need to confidently implement new technologies into their practice.

Cybersecurity 101: What You Need to Know (Cont.)

WHAT YOU NEED TO KNOW ABOUT REGULATION:

- While evaluating whether or not to implement telehealth technology in your practice, consider whether it would be appropriate to conduct or update a HIPAA security risk assessment.[v]
- Additional protections, in addition to HIPAA compliance, may be considered. Information might come into your practice through medical devices and patient apps. HIPAA may not apply to medical device manufacturers or patient apps, so physicians must be extra diligent when evaluating how to incorporate information from those sources.
- Medical devices, like computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. Medical device manufacturers and health care facilities should take steps to ensure appropriate safeguards.
- The U.S. Food and Drug Administration (FDA) does not conduct cybersecurity premarket testing for medical devices.[vi] Testing is the responsibility of the device manufacturer. Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their devices, including risks related to cybersecurity. They are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance.

[i]American Medical Association. Medical cybersecurity: A patient safety issue. Retrieved from https://www.ama-assn.org/delivering-care/patient-support-advocacy/medical-cybersecurity-patient-safety-issue

[ii]American Medical Assocation Wire. (2017). 8 in 10 doctors have experienced a cyberattack in practice. Retrieved from https://www.ama-assn.org/practice-management/sustainability/8-10-doctors-have-experienced-cyberattack-practice

[iii]American Medical Association. (2017). Protect your practice and patients from cybersecurity threats. Retrieved from https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/network-security.pdf

[iv]American Medical Assocation. (2017). How to improve your cybersecurity practices. Retrieved from https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/cybersecurity-improvements.pdf

[v]American Medical Association. HIPAA security rule & risk analysis. Retrieved from https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis

[v] U.S. Food & Drug Administration. FDA Fact Sheet: The FDA's Role in Medical Device Cybersecurity. Retrieved from https://www.fda.gov/downloads/MedicalDevices/