

Cybersecurity 101: What You Need to Know



The AMA's researchⁱ 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 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 patients' 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 physiciansⁱⁱ have experienced some form of cyberattack.
- While inappropriate employee use and disclosure of PHI (e.g., inappropriate sharing or selling of patient information) is 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 4 hours because of a cyberattack; 1 in 10 have experienced downtime of up to 2 days.

WHAT YOU NEED TO THINK ABOUT WHEN IMPLEMENTING TECHNOLOGY:

Your practice's health information technology (health IT) networkⁱⁱⁱ 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 digital health solution/service will impact your health IT network. 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:

- Cybersecurity is not just a technical issue; it's a patient safety issue.
- Implementing a new digital health technology in your practice may require you to conduct or update a HIPAA security risk assessment.^v
- However, HIPAA compliance is not necessarily enough to protect PHI. Information might come into your practice through medical devices and patient apps—for example, a remote patient monitoring (RPM) service. HIPAA doesn't apply to medical device manufacturers or patients, 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 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.

ⁱMedical Cybersecurity: A Patient Safety Issue. American Medical Association. <https://www.ama-assn.org/about/medical-cybersecurity-patient-safety-issue>

ⁱⁱ8 in 10 doctors have experienced a cyberattack in practice (2017). American Medical Association Wire. <https://wire.ama-assn.org/practice-management/8-10-doctors-have-experienced-cyberattack-practice>

ⁱⁱⁱProtect your practice and patients from cybersecurity threats (2017). American Medical Association. <https://www.ama-assn.org/sites/default/files/media-browser/public/government/advocacy/network-security.pdf>

^{iv}How to improve your cybersecurity practices (2017). American Medical Association. <https://www.ama-assn.org/sites/default/files/media-browser/public/government/advocacy/cybersecurity-improvements.pdf>

^vHIPAA Security Rules & Risk Analysis. American Medical Association. <https://www.ama-assn.org/practice-management/hipaa-security-rule-risk-analysis>

^{vi}FDA Fact Sheet: The FDA's Role in Medical Device Cybersecurity. U.S. Food & Drug Administration. <https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf>