A staggering 83 percent of physicians recently told AMA researchers that their practices have experienced a cyberattack of some type. The 1,300 physicians surveyed also said not enough cybersecurity support is coming from the government that will hold them accountable for a patient information breach.

But concise, actionable advice is available to help medical practices uncertain how to proceed with a task fundamental to protecting patient confidentiality and meeting government requirements—a security risk analysis.

An hour-long AMA webinar provides insights into why the analysis has become an important practice requirement, along with tips for turning the often-dreaded review into a manageable exercise. The professional obligation to protect patient confidentiality goes back to Hippocrates, but the legal mandate that the webinar focuses on comes from Health Insurance Portability and Accountability Act (HIPAA).

The law carries strict rules and sanctions concerning privacy, breach notification and, in this case, security. All HIPAA-covered entities are required to “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information [ePHI] held by the covered entity or business associate.”

The larger the practice, the more likely that specialized staff and resources will be available, but even the smallest medical practice must appropriately address HIPAA requirements. Done right, the risk analysis will go beyond limiting legal exposure. It can also help with meeting Merit-based Incentive Payment System (MIPS) requirements.

Practices have security responsibility for ePHI in three somewhat overlapping realms. The administrative responsibility, for example, includes rules, training and procedures. Technical requirements can be met with equipment features, such as encryption or automatic logoff.

Physical security safeguards entail addressing vulnerabilities where the ePHI exists, for example,
ensuring computer servers are in locked rooms. Security threats are not necessarily malicious, though recent AMA research underscores widespread incidence of cyberattacks on practices. In addition, HIPAA requires practices to always have access to ePHI, which may prove impossible as a result of forces of nature, like a flood or fire. They may also simply be accidental, like unintended (and unrecoverable) deletion of ePHI files.

The HHS Office of Civil Rights (OCR) monitors and enforces HIPAA compliance.

The webinar takes learners through the steps of uncovering, documenting and getting on the road to fixing security shortfalls. “OCR will not look favorably on a practice that has identified problems that they don’t address,” warned presenter Laura G. Hoffman, assistant director of the AMA’s Department of Federal Affairs.

In the webinar, she familiarizes learners with the must-follow rules of the security risk analysis, as well as when some flexibility is allowed. “It’s important to remember that the security rule does provide room for scalability and flexibility and generalization among different practices,” she said.

Often unrealized by many practices is that the security risk analysis carries a two-for-one benefit—it meets HIPAA requirements as well as a required check-off for the Advancing Care Information (ACI) component of MIPS. “Doing this well will position you for success in the ACI category,” noted Hoffman.

**5 steps, but never “one and done”**

HIPAA requirements point to five basic steps in conducting the analysis.

**Identify the scope.** This includes combining an understanding of the administrative, technical and physical security requirements with a complete inventory of all the devices in your practice that create, receive, maintain or transmit ePHI. The computers and servers that comprise the practice’s electronic health record system are obvious items, but others may not be. Modern photocopiers, for example, contain hard drives that retain images of everything scanned. Be sure to list all portable equipment storing ePHI.

**Assess the risk.** The purpose here is to identify and document potential vulnerabilities and to assess current security measures. Expect to conduct internal discussions—for example, with the office manager—and to seek external guidance on the current known risks and precautions concerning ePHI. The practice’s legal counsel, government agencies and professional associations are potential sources of information.

**Evaluate the risk.** Not all risks carry the same weight. It depends on how likely something unwanted is to happen and the anticipated impact. The webinar provides a grid that helps users rate

URL: https://www.ama-assn.org/practice-management/hipaa/5-steps-get-handle-your-practices-cyber-vulnerability

Copyright 1995 - 2021 American Medical Association. All rights reserved.
risk—medium, high, critical—based on likelihood of an occurrence and severity of impact.

For example, if the loss of an unencrypted laptop is judged probable given a practice’s operations (perhaps the practice that conducts patient home visits), and the anticipated impact is severe because of the risk of disclosure of ePHI (such as information about the patients being visited that day), then the risk is considered critical. That risk can be ameliorated with laptop encryption. Risks must also be ranked.

**Create a plan to address the risk.** “Once you rank your different risks, you want to create a work plan to address those risks,” Hoffman said. That will require documentation—for example, work plans, the responsible staff member or contractor, budgets, and target dates.

**Periodic review and updates to the risk analysis.** A general rule of thumb is once a year, given that MIPS is on an annual timetable. “A true risk analysis isn’t a one-and-done deal, it is an ongoing process, especially as practices adopt new and evolving technologies” said Hoffman.

The webinar was made possible by generous grant funding of the federal Transforming Clinical Practices Initiative (TCPI), an effort designed to help clinicians achieve large-scale health transformation through TCPI’s Practice Transformation Networks.

The AMA and HITRUST Alliance have partnered to provide small- and mid-sized practices with trusted information and strategies to effectively address these important cybersecurity issues. Workshops will be held across the country in conjunction with the recently announced HITRUST Community Extension Program. Find out about upcoming dates and locations.

**More on this**

- When is it OK to disclose PHI? HHS updates its guidance
- HHS begins second phase of HIPAA audits