A groundbreaking cybersecurity survey points to policy changes that can help physicians preserve patient safety amid widespread cyberattacks. In the meantime, there are quickly implementable steps that practices can take until the industry catches up with what physicians say they need to protect patients.

A free, one-hour webinar, “Cybersecurity: A patient safety issue,” is based on a recent AMA/Accenture, 1,300-physician survey revealing the day-to-day electronic data protection challenges faced by physicians. One key takeaway is that doctors are besieged, with eight in ten reporting having been cyberattacked. Another top finding is that physicians, by roughly the same proportion, remain positive about the potential good that can come from data sharing.

Patient safety is intertwined with both those realities. Shared patient information can be an important treatment aid, but only if it is accurate and uncorrupted, as well as quickly and reliably accessible. Theft and diversion of patient identities can result in electronic health records (EHRs) containing false information that is difficult to correct, easily resulting in compromised patient safety and care.

Hijacked records held until an electronic ransom is paid are a resource-wasting disruption at best and, at worst, a patient-endangering crisis if access is blocked in an emergency. Reliance on increasingly sophisticated, networked equipment and devices comes at a price—they, too, are vulnerable to cyberattacks.

The traditional healthcare policy response has been through practice-by-practice compliance with rules tied to the Health Insurance Portability and Accountability Act (HIPAA) and Medicare payment incentive programs. The overwhelming proportion—87 percent—of physicians believe their practices are HIPAA-compliant, but roughly the same number say they don’t think that is enough to fully protect their patient’s electronic information.

The AMA is using the survey data to look “at how we can encourage the federal government to
provide positive incentives to physicians who start to really integrate good cyber practices” when providing patient care, said webinar co-presenter presenter Laura G. Hoffman, assistant director of the AMA’s Department of Federal Affairs. Those incentives are based on the long-overlooked physician perspectives captured in the survey, combined with HIPAA’s own standards of “reasonable and appropriate” solutions in other contexts.

Many physicians already get cybersecurity compliance assistance from expert vendors. The survey indicates substantial interest in expanding those relationships, if incentivized to do so. Seventy percent of physicians would be willing to pay a vendor to implement a cybersecurity framework if adoption meant that practices would not be randomly audited under HIPAA. Another “reasonable and appropriate” incentive would be if a formal practice-vendor relationship met HIPAA and Medicare’s Advancing Care Information requirements to conduct a security risk analysis.

“Small practices in particular have really limited security resources,” noted Hoffman. Pointing to another policy proposal, she said that nearly one in two physicians in smaller practices would like to obtain cybersecurity-related hardware, software or expertise from other provider groups. But at a policy level, that would require safe-harbor exemptions from the Stark Law and Anti-Kickback Statute. Precedent for that already exists, as both already have similar provisions for the donation of EHRs.

What you can do right now

Practices should not wait for those policy responses. Co-presenter and AMA Senior Health IT Consultant Matt Reid provided a list of actions “even a solo physician practice can do within the first or second week,” of starting a cyber hygiene regime:

Protect your mobile devices. Encrypt and password-protect all of them, including mobile phones, tablets and laptops. They are easy to steal. For example, the theft rate for laptops is one every 53 seconds.

Keep software up to date. Software updates—also called “patches”—address security flaws as they are discovered and are a fundamental protection against malicious software. The need to update applies to computers and server operating systems, as well as all the software that makes practice work possible, such Microsoft Office, Adobe Reader and Adobe Flash.

Install anti-virus software. This specialized software can scan for, block, and remove computer viruses. Like software updates and patches, computers carrying anti-virus protection must be kept running and connected online to allow updates against with constantly emerging threats.

Secure your Wi-Fi network. Your Wi-Fi system touches virtually every target for a potential digital breach. The practice and patients should never share a Wi-Fi network or password. Instead, create a
guest network and password separate from the one used to connect practice devices. Make sure a firewall is running—this applies to individual computers and servers as well—that can block malware.

**Make secure passwords a priority.** Create and enforce a workplace policy requiring strong passwords, using a mixture of letters, numbers, and symbols—never shorter than eight characters. Login information should never be shared; each physician and staff member must have a unique user account name and password. When not in use, lock computer screens—on PCs, the keyboard combination is Windows key + L.

Finally, “one of the security requirements under HIPAA is to have a disaster backup plan in place,” said Reid. It is not enough to have the plan, he added, testing is also necessary to know that it works.

The webinar was part of the AMA’s Share, Listen, Speak, Learn Series (SL2), which includes an archived version of the event and links to further resources, including CME credit.

**More on this**

- 8 in 10 doctors have experienced a cyberattack in practice
- When is it OK to disclose PHI? HHS updates its guidance
- HHS begins second phase of HIPAA audits