In age of digital crime, old motto applies: Be prepared

MAR 16, 2018

Staff News Writer

Physicians should treat the possibility of a future cyberattack not as a matter of if, but when. Add to that another reality medical practices need to embrace: The time to work out a cybersecurity game plan is before—not after—an attack.

The warning about the near inevitability of a cyberattack is a message that the AMA has been spreading following the striking findings of a 1,300-physician survey the association conducted with global consulting firm Accenture.

Eight in 10 physicians reported already having experienced a cyberattack in practice. The majority fear a repeat, and many doctors appear uncertain whether they are fully prepared to protect their patients and their practices. In releasing the survey results, the AMA said, “The findings suggest a strong need for improved cybersecurity education for physicians.”

The AMA is offering two free, one-hour webinars—How to Conduct a Security Risk Analysis and Cybersecurity: A Patient Safety Issue—along with other resources on its website to give physicians and practice managers actionable advice to prevent attacks. For a broader view of what’s required to prevent and recover from a cyberattack, there are five fundamental ideas to keep in mind.

In cybersecurity, HIPAA sets medicine apart. The Health Insurance Portability and Accountability Act (HIPAA) sets stringent rules, and potentially staggering fines, which apply only to patient health information. In the event of a cyberattack, or even a nonmalicious breach, a necessary analysis is whether HIPAA-covered electronic protected health information (ePHI) is involved.

That determination can be straightforward—a laptop or even a thumb drive with ePHI goes missing—or more challenging, as in the case of a computer virus. In the event of a breach, rules concerning notification to the government, patients and even the media kick in. The scope and urgency of the reporting depends on whether the scale of the breach is above or below 500 patient records.

HIPAA spells out accountability and can help in prevention. The law requires medical practices

to regularly conduct a security-risk analysis. That entails taking an inventory of vulnerable technology—an eye-opening exercise for many practices—to assess the risk of a breach each poses. As risk is assessed and ranked, defenses can be tightened.

Even seemingly innocuous office equipment can pose a serious problem. Modern photocopiers, for example, don't just make copies; they electronically store every image that's scanned. The risk analysis is "a first step that physicians should take to ensure that they understand the scope of their network that could contain ePHI," said Laura G. Hoffman, assistant director of the AMA's department of federal affairs, and presenter on both webinars.

Prevention can fail, so a backup plan is needed. A successful cyberattack may or may not entail ePHI, but it is virtually guaranteed to involve hours or even days of workplace disruption. HIPAA requires a backup plan to regain access to ePHI and other patient information, and the elements of that preparedness can easily apply to technology that doesn't contain patient records. Elements of a recovery plan will vary by the size and resources of individual practices, but can include temporarily switching to paper files, receiving assistance from vendors or temporarily seeing patients at another office of a multi-location practice. Also, it is not enough to simply have a plan—it must be tested.

Encryption is not mandatory, but you'll regret not having it. HIPAA does not explicitly require it, but encryption of ePHI is fundamental protection for patient safety and privacy. It also provides important legal protection to the practice. For example, if a laptop with encrypted ePHI is stolen, the records within cannot be accessed and misused—in short, it's not a breach.

The security-risk analysis will help point a practice to devices that are most at risk, and anything portable should be at the top of every practice's list. "Make sure you have efficient and sufficient encryption of your ePHI," Hoffman said.

A cyberattack is a learning experience. Cybercrime endures not only because it is highly profitable—and medical records are among most valuable data to steal—but because cybercriminals are constantly honing their skills. Practices have to take the same approach to protection. Any time a practice is cyberattacked—even a near miss with no damage done—it is important to re-examine and update security protocols.

For example, sophisticated sham emails to steal passwords or launch malicious software—so-called phishing attacks—often target health care settings. Spam filters might catch most of them, but knowing how not to fall for those that get through requires training and vigilance. In the wake of any cyberattack, practices should "learn from what happened, recover, and get back up on your feet," said AMA Senior Health IT Consultant Matt Reid, co-presenter of the patient safety webinar.

He added that it is also important to share those lessons learned with others in the medical community: "Say, 'Look this happened to us,' and help others understand what your experience was,

so they don’t go down the same path.”

Looking ahead, the AMA is exploring how practices can be incentivized to work closer with vendors on cybersecurity. Nearly three-quarters of the doctors in the AMA-Accenture survey said they would be willing to pay a vendor to implement a cybersecurity framework if adoption meant that practices would not be subject to random HIPAA audits.

Also on the AMA’s advocacy list: safe-harbor exemptions from the Stark Law and Anti-Kickback Statute expanded to allow donation of cybersecurity-related hardware or software to small medical practices from other provider groups. The AMA recently sent a letter to the U.S. Department of Health and Human Services’ Office of Inspector General on the matter.

In the letter, the AMA expressed its deep concern that the country’s health care providers have been insufficiently prepared to meet the cybersecurity challenges of an increasingly digital health system. The AMA firmly believes that this is a national priority and that physicians and other health care providers need tools to secure sensitive patient information in the digital sphere.