To beat digital divide, time for “the talk” with your IT vendors

MAR 12, 2018

Staff News Writer

Medicine has its own version of a digital divide. In terms of cybersecurity accountability, the buck stops with the physician. The problem is that security expertise lies with information technology (IT) vendors who provide software, equipment, training and other services to physician practices. These vendors often speak a different language than the physician, who is well versed in clinical matters but whose tech savvy may end with the cable TV remote.

“Physicians are not security experts. It’s not what they went to school for,” said Laura G. Hoffman, assistant director of the AMA’s department of federal affairs, and presenter on two recent AMA cybersecurity training webinars. Because physicians are not experts, they “rely on their health IT vendors for support and security guidance.”

A recent AMA-Accenture survey of 1,300 physicians found that more than a quarter of physicians already outsource their security management and an almost equal number are interested in doing so. Many physician practices go it alone—about half of the practices surveyed have an in-house security official—juggling the requirements of various systems and equipment, and relying largely on trust that the products and services they pay for are secure, reliable and work seamlessly together.

“Physicians really trust their vendors and that can be good and bad,” Hoffman said. Under the Health Insurance Portability and Accountability Act (HIPAA), she noted, it’s physicians who “are the ones on the hook if anything goes wrong.”

Bridging medicine’s cybersecurity digital divide can be an intimidating prospect, especially for smaller practices. How products from various vendors fit together may be unclear. The scope of a physician’s discussion with a vendor will vary greatly by not only by practice size, but by technology choices. For example, a practice with cloud-based records storage will have different concerns to address than one with its own server. Here is what to consider for having a more effective conversations with vendors.

Think ePHI and beyond, not just EHR. A medical practice’s starting point for getting a handle on vendors might be the electronic health record (EHR), but cybersecurity preparedness and
accountability requires a broader view. In terms of cybersecurity, HIPAA covers any and all electronic protected health information (ePHI). An EHR is sure to contain ePHI, but ePHI is likely to be found throughout the practice. HIPAA requires a security risk analysis and whether done in-house or by a vendor, it is a great starting point for getting an inventory of all the relevant technology and understanding the interactions of the devices involved.

The AMA offers a free, one-hour webinar to familiarize physicians and practice managers about how to conduct it. Beyond obvious HIPAA concerns, there is other technology—for example, non-EHR office software and computers—that can play a role in the safe and smooth functioning of the practice. “Identifying the actual technology in your environment is a first step in making sure everyone is at the table when you have these conversations,” said AMA Senior Health IT Consultant Matt Reid, co-presenter with Hoffman in a separate AMA webinar on cybersecurity and patient safety.

**Practices need to be more assertive.** Technology from different vendors may not always smoothly mesh. For example, a larger practice with cloud-based records storage requires an Internet service provider to supply sufficient Internet bandwidth to reliably store and retrieve data.

What’s required is a practice cybersecurity and technology “champion,” said Reid. It is that individual—who may well be a practice staff member as opposed to a physician—who can get vendors together, face to face or in a conference call, to have all the practice’s technology work together. According to Reid, the champion’s message should be: “This is an issue where we all want to row in the same direction, so how are we all going to work together cohesively?”

**Vendors need to be more forthcoming.** When that practice champion gets the conversation going, a top priority is collecting and sharing a complete set of technical information from all of the practice’s health IT vendors. The objective is to find out fully what the practice needs to know about and, critically, what the vendors need to know about each other’s hardware, software and services requirements.

**Testing is essential.** A practice should periodically test the technology it relies on—Hoffman noted one example of an EHR that, unbeknownst to the practice, ran out of storage space—and be aware that technology problems can arise whenever anything new is added to the mix.

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.

More on this

- What you can do about patient safety’s latest threat—cyberattacks
- 8 in 10 doctors have experienced a cyberattack in practice