PRACTICE MANAGEMENT

8 in 10 doctors have experienced a cyberattack in practice

DEC 12, 2017

Staff Writer
AMA Wire

Physicians, overwhelmingly, are finding themselves the target of cyberattacks that disrupt their practices and put patient safety at risk.

A staggering 83 percent of physicians 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. These and other findings are contained in a first-of-its-kind survey from the AMA and management consulting firm Accenture. The data (infographic) provide new depth—and an often overlooked physician voice—to the discussion on how best to protect patients in a complex health care system that is increasingly connected and vulnerable to cybercriminal exploitation.

"The important role of information sharing within clinical care makes health care a uniquely attractive target for cyber criminals through computer viruses and phishing scams that, if successful, can threaten care delivery and patient safety," said AMA President David O. Barbe, MD, MHA. "New research shows that most physicians think that securely exchanging electronic data is important to improve health care. More support from the government, technology and medical sectors would help physicians with a proactive cybersecurity defense to better ensure the availability, confidentially and integrity of health care data."

A June 2017 report by the congressionally mandated Health Care Industry Cybersecurity Task Force found "health care cybersecurity is a key public health concern that needs immediate and aggressive attention," and that, "most importantly, cybersecurity attacks disrupt patient care." The 88-page document underscores the risk to medical care delivered in smaller settings, which are especially vulnerable to attacks by cybercriminals.

Most of the AMA survey respondents report being either very or extremely concerned about future attacks aimed at their practices. All practice settings are at risk, but attacks are twice as likely at medium- and large-size practices. Malware—the broad term for a wide range of malicious software—is a top concern, as are breaches involving the theft of electronic patient health information.

Nearly three-fourths—74 percent—of the respondent physicians said that interruption or inconvenience to the running of their practices is their greatest concern. In the context of medical care, that business disruption can very quickly become a patient safety concern. Phishing attacks also are among the top threats cited by physicians. The technique involves the use of often very sophisticated sham emails to entice recipients to reveal sensitive information—such as passwords—or trigger malware, including ransomware that blocks access to patient records and other viral practice information until an untraceable online payment is made. (More about the survey.)

Related Coverage
5 things to know about HIPAA and cloud computing

Other cybercriminals just want to steal patient information outright. Medical files are highly valued in the world of financial fraud because of the depth of information they contain, far more exploitable than just a credit card number hacked from a retail site. But, increasingly, the concern is that patient information will be used in a wide variety of health care fraud. Fake claims to defraud payers also place false diagnosis and treatment information into the medical record of the legitimate patient whose data were hijacked. It is not only patient files that are at risk. Another serious concern, still mostly on the horizon, is the hacking through online connectivity and malware of medical devices—the FDA recently recalled nearly a half-million pacemakers because of that vulnerability—critical to patient care.

Still, there is no turning back on the positive uses of the technology and the AMA survey reports that 85 percent of the respondents believe it is important to have the ability to share patient electronic information. But they are critical of the public policy implementation that, after they were encouraged to go online, frustrates them when it comes to meeting the accountability standards Washington has set.

Cybersecurity's big practice costs

Meaningful use incentives—now part of Medicare's Merit-based Incentive Payment System—put many physician practices on the road to online connectivity. The privacy enforcement standards under Health Insurance Portability and Accountability Act (HIPAA) set substantial penalties for violations. However, the complexity of HIPAA compliance has left physicians in a quandary—how to comply with elaborate requirements, explained in dense legalese, when the application of the law is in the real-life world of patient care.

The vast majority of physicians—87 percent—believe their practices are HIPAA compliant, but 83 percent believe HIPAA compliance is "insufficient." They want to understand where their practice is at greatest risk so that attention and investment can be directed there. Many physicians say they want tips for good cyber hygiene, simpler legal language on HIPAA requirements, how-to advice on conduct cybersecurity risk assessments, and information on what to consider before hiring a consultant to help with HIPAA compliance.

Meanwhile, practices are running up six-figure annual cybersecurity bills. The amounts can be $250,000 per year for a nine-physician practice, or as much as $400,000 annually for a regional medical center with 50-plus physicians. To make the most effective use of the spending, it is important to establish a cybersecurity risk-management program. The AMA has partnered healthcare cybersecurity alliance HITRUST to help small- and mid-sized practices with dependable information and strategies, in a series of workshops in eight cities throughout the country, including Pittsburgh, Chicago, Cleveland and Dallas. See the complete list of upcoming dates and locations.

Physicians can get a quick start on understanding the issues with the AMA's one-hour cybersecurity webinar Jan. 24, 2018. Online attendees will be informed on what the AMA is doing about awareness and understanding on the issue, and how physicians can advocate to protect their patients and gain insights into the shared responsibility for securing electronic patient information. Register.

More on this

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

Health IT Physician Advocacy