5 things you didn’t know about health care cybersecurity

OCT 10, 2019

Andis Robeznieks
Senior News Writer

Criminals value medical files because of the amount of exploitable financial and personal information they contain and the growing potential that exists to use the data in a wide variety of fraud schemes.

The AMA offers physician cybersecurity tips to protect patient health records and other data from cyberattacks.

Cybercriminal schemes include defrauding payers by putting false diagnosis and treatment information into the record or hacking into systems, bypassing medical device cybersecurity measures in a way that could threaten patient care.

A survey of 1,300 physicians conducted by the AMA and the Accenture consulting firm revealed five key findings that doctors need to know to help safeguard their practices.

Cyberattacks are common in clinical practices

More than four out of five physicians have been a victim of some type of cyberattack, with “phishing” being the most common (55%).

Phishing uses 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 vital practice information until an untraceable online payment is made. Nine percent of respondents reported that their practice’s information was held in a ransomware scheme.

The next most common attack involves computers being infected with viruses or malware via a downloaded file.

Cyberattacks cause operational interruptions

Both electronic health record (EHR) security breaches where patient data was compromised and interruption of practice operations because EHR access was blocked were cited by 74% of responding physicians as a top cybersecurity concern.

One in three physicians said their practice experienced a cyberattack-related business shutdown. Here is how long these physicians' practice systems were down:

> Four hours or less: 64%.
> Five to seven hours: 20%.
> One to two days: 12%.
> More than two days: 4%.

Most physicians think sharing information is important

Eighty-five percent of physicians believe sharing electronic protected health information was "very" or "extremely" important.

But integrated care arrangements are only as strong as their weakest link. To securely share data, physicians need to work together and practice good "cyber hygiene" to protect the entire electronic health care ecosystem.

The AMA advocates that the federal government offer positive incentives—not just penalties—to encourage physicians to bolster their security systems. Incentives could include creating Improvement Activities within Medicare's Merit-based Incentive Payment System (MIPS) that provide credits for implementing good cybersecurity practices.

Physicians rely on third-party cybersecurity assistance

Almost half of physicians have an in-house security official, but only 20% of small practices do and they typically trust health IT vendors to provide cybersecurity support. About one-quarter of physicians outsource security management and 28% said they do not, but are interested in doing so.

Seventeen percent have received donated security-related hardware or software from other provider groups, hospitals or health systems. Another 29% have not received such donations, but are

interested in receiving them. The AMA is working on ways to help physicians receive these donations while remaining in compliance with laws and taking proper cybersecurity measures.

The AMA advocates increased support from the federal government to help practices bolster their breach resilience. A new AMA-endorsed law directs federal agencies to dedicate cybersecurity resources to small business—including physician practices.

Physician cybersecurity resources

Half the physicians surveyed also said they would like to receive tips on good cyber hygiene. To help them, the AMA has developed tips and advice on protecting your computers and network to keep your patient health records and other data safe from cyberattacks.

- How to improve your cybersecurity practices (PDF)
- Cybersecurity checklist for office computers (PDF)
- Protect your practice and your patients from cybersecurity threats (PDF)
- Infographic: Cybersecurity in health care (PDF)

A safety checklist for office computers is also available.

The AMA Digital Health Implementation Playbook has a cybersecurity 101 section on basics that physicians need to know. These include key messages that cybersecurity is not just a technical issue, but a patient safety issue, and that most small practices rely on third-party vendors for cybersecurity support.

The webinar, “Cybersecurity: A Patient Safety Issue,” reinforces the importance of cybersecurity to patients and discusses how the AMA is shaping the national cybersecurity conversation to focus on patient safety.

Recent research published in *JAMA Network Open*, “Assessment of Employee Susceptibility to Phishing Attacks at U.S. Health Care Institutions,” found that there was a 16.7% median click rate at six hospitals where simulated phishing emails were sent to employees. The study also notes that awareness campaigns were linked to decreased odds of clicking on a subsequent phishing email.

Previous research published in *JAMA*, “Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010-2017,” delved into the 2,149 breaches reported to the Department of Health and Human Services between 2010 and 2017.