Physician cybersecurity

Updated Aug. 31, 2021

Cybersecurity overview

Viruses, malware and hackers pose a threat to patients and physician practices. The AMA has curated resources and has tips for physicians and health care staff to protect patient health records and other data from cyberattacks.

Protecting electronic health information

Electronic health records are enhanced versions of traditional medical records—making information available instantly and securely to authorized users. Most electronic health record (EHR) systems have security features built in or provided as part of a service. Yet, they are not always configured or enabled properly. This can lead to unauthorized access to your patients' electronic health information. It is important to learn about the basic features of your EHR and ensure they are functioning and are updated when necessary. Health care organizations—along with their EHR vendors—should make protecting their EHRs from cyber threats a top priority in order to keep their patients safe and secure. This document developed by the U.S. Department of Health and Human Services (HHS) (PDF) lists several resources that can strengthen the cybersecurity in your medical practice.

Ransomware and email phishing attacks are on the rise

Ransomware is a form of malicious software designed to encrypt files on a computer or other device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak data (e.g. business and patient records) or authentication information (e.g. usernames and passwords) if the ransom is not paid. This is particularly concerning if a health system's EHR or other medical technology is infected. In recent years, ransomware incidents have become increasingly prevalent among health care organizations.

A main conduit for ransomware is your office's email systems. Email is the preferred attack vector for malicious phishing campaigns. By mentioning current events, threat actors carrying out attacks can craft emails that are likely to capture recipients' attention and lure them to click a link or download a file containing malicious code—this is referred to as phishing. Given the recent shift to more telework and remote options, organizations and workers face increased risk of falling victim to phishing emails and cyberattacks.

The HHS and the U.S. Cybersecurity & Infrastructure Security Agency (CISA) have created resources and guides to help medical practices and other small business protect against ransomware and phishing:

- Counter Phishing Guide (PDF)
- Ransomware (PDF)

Picture Archiving Communication Systems (PACS) Vulnerability

Picture Archiving Communication Systems (PACS) are widely used by hospitals, research institutions, clinics and small health care practices for sharing patient data and medical images. In 2019, researchers disclosed a vulnerability in these systems that if exploited could potentially expose patient data. PACS servers are easily discoverable by attackers using simple open source scanning tools. If left unpatched, these systems can expose patient records to unauthorized access. Infected PACS servers can also compromise connected clinical devices and spread malicious code to other parts of your office network. There continues to be a number of unpatched PACS servers still in use today.

The AMA recommends that physicians reach out to their PACS vendors about patching their systems. More information about this vulnerability can be found on this Health Sector Cybersecurity Coordination Center alert (PDF).

Technology considerations for the rest of 2020

A resource from the AMA and the American Hospital Association provides steps physicians should take (PDF) to prepare for the coming months as many physician practices are or have reopened, including cybersecurity and privacy considerations.

HHS launches new cybersecurity website

The Department of Health and Human Services' (HHS) Health Sector Cybersecurity Coordination Center (HC3) has recently launched a new website to help physicians and their medical practices be better informed about potential cyber threats.

HHS is working with practitioners, health care organizations and cybersecurity experts to understand the threats facing the health care sector, learn the patterns and trends used by malicious actors, and provide information and approaches on how the medical practices and hospitals can better defend themselves.

This new site lists several resources, including:

> Threat briefs with best practices and information on COVID-19 related cyber threats
> Sector alerts with high-level information to assist non-technical audiences

Guide for working from home during the COVID-19 pandemic

Responding to a spike in cyber threats that exploit telework technologies during the COVID-19 pandemic, the AMA and the American Hospital Association (AHA) teamed up to provide physicians and hospitals with guidance on protecting a remote work environment from cyber criminals.

"Working from home during the COVID-19 pandemic" (PDF) offers actions to strengthen home or hospital-based computers, networks and medical devices from the rise in COVID-19-themed security threats and attacks. The resource includes checklists, sources, tips and advice on strengthening protections to keep pace with deceptive cyberattacks that could disrupt patient care or threaten medical records and other data.

Creating an informative e-mail campaign

In an effort to spread awareness of cybersecurity across your organization, a packet of infographics, images and posters have been developed along with simple instructions to help you create an informative and engaging email campaign. The email campaign instructions and images can be found in the NCSAM Package.

Additionally, health care and security experts have developed a set useful materials to help guard

your entire medical practice against cyberattacks. These materials have been designed with small to medium-sized medical practices in mind.

The main document (Health Industry Cybersecurity Practices) explores the five most relevant and current threats to physician offices and recommends 10 cybersecurity practices to help mitigate these threats. Technical volumes 1 and 2 provides the “how” so physicians and office administrators can implement these practices in their small, medium or large health care organizations.

Digital health technology adoption requires medical cybersecurity

According to a first-of-its kind survey, physicians are greatly concerned about the theft of private patient information and loss of access to critical medication lists, diagnoses and lab results.

The research also showed the physician perspective is often missing from many major cybersecurity efforts.

The AMA is well-positioned to better include the physician input in cybersecurity efforts going forward.

Medical cybersecurity issues

The main findings identified three key themes:

1. Cybersecurity Is a patient safety issue.
2. Physician practices rely on health IT vendors for network and system security.
3. HIPAA compliance Is not enough to protect patient records.

Physician cybersecurity resources

The AMA has also developed tips and advice on protecting your computers and network to keep your patient health records and other data safe from cyberattacks.

Download and share with your staff and IT:

> Technology considerations for the rest of 2020 (PDF)
> 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)
- Working from home during COVID-19 pandemic (PDF)

Cybersecurity improvements

The AMA continues its work to improve health care cybersecurity.

- AMA letter to OIG on “Solicitation of new Safe Harbors and Special Fraud Alerts" (PDF)
- AMA letter to Congress on cybersecurity and the use of legacy technologies in health care (PDF)
- AMA letter to FDA on "Developing a Software Precertification Program: A Working Model" (PDF)
- AMA statement to FDA on intersection of big data, privacy and competition (PDF)