# What doctors can do to thwart cybercriminals as 2020 closes

NOV 10, 2020

**Andis Robeznieks**
Senior News Writer

A resurgence of COVID-19 combined with the flu season will add up to a growing reliance on digital tools in an effort to provide patients care while letting them stay in their homes.

To help physicians and others prepare, the AMA and the American Hospital Association (AHA) have developed a resource that includes recommended steps needed to bolster network security and patient privacy efforts.

The resource, “Looking Forward: Technology Considerations for the Rest of 2020,” builds on and updates a previous AMA-AHA joint resource “What Physicians Need to Know: Working from home during the COVID-19 pandemic.”

“Privacy and security are distinct, but closely interrelated,” the resource says. “It is not enough for medical practices and hospitals to invest in one but not the other. Fortunately, the concepts are mutually reinforcing, meaning that many actions that are taken to bolster security of patient information will also better protect the privacy of that information.”

While fighting to contain the pandemic, physician practices and hospitals have also had to combat cybercrime on these three fronts.

**A “dramatic” rise in phishing campaigns.** Emails promising needed equipment that was in short supply—from N95 masks to ventilators—flooded the health care sector. But, behind these empty promises were malware and malicious links.

**Targeted attacks on vulnerable links between patients and physicians.** Cyber criminals struck the virtual private networks and other cloud services that were brought into use for telehealth and medical remote-monitoring devices.

**Ransomware attacks are a growing concern.** These can be particularly harmful because they can disrupt patient care, disable critical systems, interrupt revenue flow, necessitate the installation of expensive remedies, and put institutions and practices at risk for legal and regulatory exposure and

reputational harm.

Learn more about how online scammers target doctors amid COVID-19 and how to stay safe.

## Strengthen network connections

While enhanced interconnectivity can benefit patients by supporting integrated care, it also makes systems especially vulnerable as a successful attack on an individual network component can have rippling negative impacts among physician offices, hospitals, ambulatory surgery centers, laboratories, pharmacies and imaging centers.

The resource's section on security includes several questions that physicians and others need to answer. These are among them.

**Are there network components that may create vulnerabilities?** These may include personal mobile devices or home computers with out-of-date firewall technology.

**Are there legacy devices that use Windows 7 as their operating system?** Unless an extended security update was purchased, support for Windows 7 expired early this year, meaning no further security updates are forthcoming.

**Where is protected health information (PHI) stored?** The resource recommends actions be taken if PHI is sent via unencrypted emails or knowingly or unknowingly stored in medical devices or office equipment. Photocopiers, for example, can store thousands of patient records.

## Ensure that vendors protect privacy

In an effort to spur use of telehealth at the start of the COVID-19 public health emergency, the U.S. Department of Health and Human Services Office for Civil Rights announced that it would use discretion in enforcing HIPAA privacy and security violations for physicians and hospitals who made a good faith effort to quickly adopt telehealth technology to connect with their patients.

This discretionary period will likely close, however, with the end of the declared emergency, so the resource advises physicians to start planning now on how they will come into HIPAA compliance if they are not already.

On both the cybersecurity and privacy fronts, a strong business associate agreement (BAA) with vendors is key and the BAA should match the level of risk associated with the vendor's role, amountof data they hold, the sensitivity of that data and the vendor's access to it.

"Many physicians do not realize that a telemedicine platform or application may be low-cost or free because the vendor's business model is based on aggregating and selling patients' data," the resource states. "If possible, consult with your legal team to clarify how video, audio, and other data are being captured and stored by the vendor and who has access."

The AMA has also curated resources and tips for physicians and health care staff to protect patient health records and other data from cyberattacks.