Cyber vulnerability grows along with COVID-19 pandemic stresses

NOV 30, 2020

Len Strazewski
Contributing News Writer

As the COVID-19 pandemic rages, demand for telehealth services has also grown, increasing the vulnerability that medical operations have to cyberattacks and hacks, according to Laura Hoffman, AMA assistant director of federal affairs.

Hospitals and medical practices must always take steps to protect their networks from cyberattacks on patient records and other data, but as hospitals and physician practices have adjusted to provide more care virtually, while also devoting significant resources to treating patients with COVID-19 and managing the increased number of cyberattacks on health care providers, security can become stressed, she said during a recent episode of the “AMA COVID-19 Update.”

“In the pandemic, we rightfully have a lot of resources focused on caring for patients with COVID. So, you've got a lot of additional personnel maybe working in different areas of the hospital that they aren't accustomed to, maybe their access controls have had to change in terms of who's allowed out into what portions of the electronic health records, and that can contribute to insider threats,” Hoffman said.

“We've got people continuing to work from home and continuing to receive treatment from home. So, the landscape of the vulnerabilities and entry points during the pandemic are increased as compared to a regular health care system where a lot of the care is delivered inside your secure clinic or hospital.”

To help physicians and others manage these issues, the AMA and the American Hospital Association (AHA) have developed a resource, “Looking Forward: Technology Considerations for the Rest of 2020 ,” that includes recommended steps needed to bolster network security and patient privacy efforts.

Telehealth creates vulnerabilities

Hoffman also pointed to a growing reliance on telehealth and how more patients are receiving care from home using different telehealth platforms. The use of the technology has been “a wonderful way for us to promote social distancing and preserve” personal protective equipment (PPE), she said.

“But at the same time, what is good for the health care system and patients presents an opportunity, unfortunately, for cyber criminals. So, they see this now as an opportunity to perhaps exploit these increased use of telehealth systems and the fact that people are working in an environment that they may be less familiar with, and they are going to town in terms of trying to infiltrate different systems,” Hoffman said.

Ransomware, a long-standing problem for individual internet users, is also on the rise for institutions.

“In the beginning [of the pandemic] we saw a lot of attacks via phishing and ransomware. Having people click on links for additional PPE that they might be trying to find ... actually would then infect computers and systems,” she said.

Ransomware criminals then demand money from affected institutions to release infected software and locked up data. “It's not just something that happens in a back room where the IT staff then gets busy to work and trying to fix the ransomware that has infected the system,” Hoffman noted. “It really is a system-wide impact when your systems are shut down. You can't pull up distinct patient records to learn what medications they're on or even what their diagnoses are.”

Beware of insider threats

One of the newest and biggest threats is called “Ryuk ransomware,” she explained, which has been released into the open internet for use by any malicious criminal.

The ransomware has created an opportunity for insider attacks by individuals who recognize an opportunity to exploit weaknesses in an institution’s technology.

“We're seeing a lot of insider threats, unfortunately, where folks may recognize that their systems aren't patched as strongly as they should be or completely as they should be, and they're able to just insert this software right into some unsecured systems. One of the biggest examples we've actually seen recently is with the UHS [Universal Health Services Inc.] health care system where computers were infected, and many practices had to shut down. Hospital systems were without their EHR for some time,” Hoffman said.

It's not just hospitals and large institutions that are affected. Small practices or individual physicians working from home may be storing less data, “but they may not have the same kinds of robust cybersecurity protections in place, and so it's easier to infiltrate that network and maybe link it to a larger network,” she said.

Keep software up to date

Hoffman recommends IT staff check that software is up to date and make sure software patches for all technology are completed regularly—even personal computer operating systems and internet browsers that link to bigger data management systems.

“One thing to consider is giving all of your employees a really serious refresher about the kinds of links they should be clicking on when they review their emails inside the hospital system. Maybe have everybody change their passwords more frequently, make the requirements more complex.

“I know it just adds one more thing for everybody to remember, but you can use password managers to help with that and come up with complex passwords that you don't need to actually remember every time,” she said.