How the Right Technologies Can Help Manage Security in Telemedicine

As telemedicine use continues to grow, having the right devices and technologies to address security issues is now more important than ever

As COVID-19 started to spread, healthcare organizations across the country quickly implemented telemedicine applications to find ways to both serve their patients – particularly those in higher risk populations – while also protecting staff and patients from potential infection. While adoption lagged prior to the pandemic, the combination of need and relaxed regulations regarding its use accelerated telemedicine's expansion among health systems, hospitals and provider practices. In fact, in a survey conducted by the online physician network Sermo, 85% of the 1,300 physician respondents reported they were using different telemedicine platforms in response to the crisis. Perhaps more importantly, however, was the discovery that 60% planned to continue seeing patients via telephone or video chat after the pandemic subsides.[1]

"For telemedicine acceleration to continue, hospitals need to put security front and center. And, to do that … providers need to find a happy medium – a platform flexible enough to hold telemedicine appointments ... that are easy for everyone to access, but secure enough to protect their information and the enterprise as a whole."

Michael Castorino | Head of Global Strategic Healthcare Alliances | HP Inc.

Telemedicine is not a new concept – and it has long been lauded as a way to increase accessibility and convenience to healthcare. Yet, its rapid growth during the COVID-19 pandemic raises vital questions about how to protect healthcare networks and coveted patient health information (PHI) as it is used.

"When you are talking about telemedicine, security is a huge concern," said Jeffrey Goldstein, MD, Senior Healthcare Specialist at HP. "All of a sudden, your network is now connecting up with all these disparate devices so patients can receive care. Maybe those devices are smart phones, or gaming computers, or just someone's work laptop with a webcam. But, they are outside your sphere of control – and they are creating a remarkable number of insecure endpoints that your information technology (IT) people are going to have to manage in order to protect the enterprise."

Novel virus, continued threats

Unfortunately, while COVID-19 has shut down much of the country, it has not shut down the virtual bad actors hoping to gain entry into healthcare organization networks. In fact, the U.S. Department of Health and Human Services (HHS) reported an almost 50% increase in reported data breaches between the months of February and May this year.[2]

For most people seasoned in the healthcare security world, the uptick in attacks is not much of a surprise, according to Goldstein. Hackers who are able to successfully access patient medical records have financial incentive to do so.

"If a hacker gets hold of your credit card, it's only worth a few pennies – because once your bank or you notice it was compromised, you can cut it off and the hacker can't use it anymore," he said. "But, your medical record is worth a couple of hundred dollars. It is full of all kinds of valuable information, ranging from insurance to health information, that can potentially be leveraged again and again. This stuff needs to be protected."

While regulations regarding appropriate telemedicine use may have been relaxed, the penalties for not complying with the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA) have not. Despite the fact that provider organizations have had to quickly adjust to remote methods of providing care, they remain wholly responsible for protecting their networks and PHI, according to Michael Castorino, Head of Global Strategic Healthcare Alliances at HP. Those who don't will find their names displayed on the HHS' Office for Civil Rights (OCR) breach portal, better known in the business as the "Wall of Shame." They will also potentially pay millions of dollars in related fines.[3]

"With this pandemic, providers started using all different types of platforms without taking the time to assess whether they were secure or not – and that led to data breaches," he said. "For telemedicine acceleration to continue, hospitals need to put security front and center. And, to do that with all these different telemedicine applications, providers need to find a happy medium – a platform flexible enough to hold telemedicine appointments with patients that are easy for everyone to access, but secure enough to protect their information and the enterprise as a whole."

Castorino added there are many challenges in keeping telemedicine offerings secure, ranging from the ability to inventory and assess the different endpoints connecting to the network to protecting all data as it is transmitted, aggregated and shared at the point of care. Each of the requirements necessary for successful telemedicine bring with them specific security issues that healthcare organizations need to effectively manage in order to avoid data breaches, network intrusions and potential threats to patient safety.

"What you want are end-to-end solutions for the healthcare enterprise that make you as secure as possible as all this data starts moving across the network with different telemedicine applications," Goldstein said. "This starts with having devices that were built to be as secure as possible. But you need security tools that allow you to identify, isolate and contain any attacks that may be coming your way, too."

"What you want are end-to-end solutions for the healthcare enterprise that make you as secure as possible. … This starts with having devices that were built to be as secure as possible. But you need security tools that allow you to identify, isolate and contain any attacks that may be coming your way, too."

Jeffrey Goldstein, MD | Senior Healthcare Specialist | HP Inc.

1. Supporting security with HP hardware

Healthcare organizations can more successfully manage telemedicine-related security issues by investing in hardware designed with security in mind, according to Castorino. He said that HP products, including the EliteOne Healthcare All-in-One (AiO) personal computers (PCs), as well as the EliteBooks and Engage devices, come standard with hardware-enforced security features, offering protection below, in and above the operating system (OS).

"We have hardware specifically developed in the BIOS to deal with security – and we have security both in the OS and above the OS," he said. "We protect the whole enterprise at the edge. It doesn't matter what kind of device our hardware is connecting up to. Having those extra layers of security in the HP devices allows you to identify and recover from attacks and, in doing so, protect the whole network."

HP devices are also designed to prevent what is known as *visual hacking*, or the act of viewing or capturing sensitive or confidential information for unauthorized use. HP Sure View, an integrated privacy screen developed in partnership with 3M, enables users to adjust the viewing angles on your computer to keep the information on your screen protected from prying eyes.

"You want the devices you are using to have that kind of visual security," said Goldstein. "Because if I'm looking at your chart, and someone is walking by me in the hospital, it doesn't take that much for them to get a glimpse of your PHI. They might also see my password or other identifying information. You want the ability to shield that information, as much as possible, from anyone else, so it isn't used in ways it shouldn't be."

2. Supporting security with HP software

Good cybersecurity, however, doesn't begin and end with the devices. It's also important to have the right cloud-based applications to help monitor and manage the network – especially as telemedicine platforms expand the number of potential endpoints that exist outside the four walls of the hospital. HP's Sure Suite products, including HP Sure Admin, HP Sure Sense, HP Sure Click, HP Endpoint Security Controller, HP Sure Start, HP Sure Run and HP Sure Recover can all help IT staff identify and mitigate potential network intrusions before they happen.

HP's Sure Suite of products helps IT staff identify and mitigate potential network intrusions *before* they happen.

"You don't want to wait until some hacker is connected to your system to protect yourself," said Castorino. "You want to be able to catch them while they are making the attempt – so you can be sure the enterprise remains secure and a breach doesn't happen at all."

With hundreds of thousands of new malware variants created each day, traditional antivirus applications can't offer adequate protection, according to Castorino. But, HP Sure Sense, an innovative cloud-based application that uses proprietary deep learning algorithms to recognize malware, can help provider organizations identify potential threats before they wreak havoc on your network.

"This is a deep learning algorithm that offers real-time, proactive protection against malware attacks," he said. "It can find the different attacks that are already out there – as well as the ones that haven't been tried yet. It gives healthcare organizations a real advantage in this fight against bad actors."

"You don't want to wait until some hacker is connected to your system to protect yourself. You want to be able to catch them while they are making the attempt – so you can be sure the enterprise remains secure and a breach doesn't happen at all."

Michael Castorino

Security in the age of telemedicine

Goldstein said there is little doubt that telemedicine applications are here to stay. While acceleration may have occurred due to COVID-19, the benefits of such platforms will ensure they will remain an important part of healthcare delivery in the future.

"There are a lot of good reasons to continue telemedicine and remote patient monitoring after this virus is gone," he said. "But, you want to make sure that you are doing everything you can to make sure your network is protected and secure as these different applications continue to evolve. The technologies are changing. The attacks are changing. And, that's why we are constantly working to improve our hardware and software to make sure that security is always at the heart of our products. We want to make sure that healthcare organizations can continue to provide patients what they need, when they need it – but do it in the most secure way possible."

To learn more about how HP devices and technologies can help make your organization's telemedicine use more secure, visit hp.com/go/healthcare.

"The technologies are changing. The attacks are changing. And, that's why we are constantly working to improve our hardware and software to make sure that security is always at the heart of our products. We want to make sure that health-care organizations can continue to provide patients what they need, when they need it – but do it in the most secure way possible."

Jeffrey Goldstein, MD

References

1. Sermo Team. 2020. Telemedicine explodes in these uncertain times. *Sermo Blog*. April 16. https://www.sermo.com/blog-telemedicine-explodes-in-these-uncertain-times/.

2. Hackett M. 2020. Number of cybersecurity attacks increases during COVID-19 crisis. *Healthcare Finance News*. June 4. https://www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis.

3. U.S. Department of Health and Human Services Office for Civil Rights. 2020. Breach portal. [Accessed July 19, 2020] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

About HP

HP is reinventing solutions to connect human intuition, compassion and knowledge for the next generation. Our technology solutions power patient interactions all over the world, and consistently evolve to advance the human connection on safer, smarter, secured technology platforms. Learn more at hp.com/go/healthcare.

4AA7-8316ENUS, August 2020

Produced by HIMSS | www.himss.org | ©2020