COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 5. May 07, 2020 Telehealth Programs Implemented in Pandemic Rush Could Be Security Risks

By Jane Anderson

Many health care organizations are racing to implement or augment telehealth services as the COVID-19 pandemic has upended medical care. But a cybersecurity expert is warning HIPAA covered organizations not to skimp on security as they rush to provide care remotely.

"Like all connected technologies, telehealth is not immune to security and privacy risks," said George Jackson Jr., senior principal consultant at health care cyber-risk management firm Clearwater. "Cybersecurity issues like hacking can adversely impact patients' or providers' level of willingness to trust telehealth. Digital health care has been plagued by several large-scale and high-profile data breaches over the years, and there's no evidence that this is going to let up."

Jackson told attendees at a webinar[1] that he views telehealth as "simply providing health-related services at a distance" and telemedicine as a subset of that related specifically to the practice of medicine remotely, governed by state laws and specific states' medical boards.

Telehealth, with telemedicine as part of it, was among the fastest-growing fields in modern health care even prior to COVID-19, Jackson said. As the pandemic has unfolded, "telehealth was given a hard shove downhill," leading to rapid growth and accelerated adoption of the technology, he said.

"Prior to COVID-19, telehealth was already well on its way to becoming a core part of the global health care infrastructure—experts even last year were predicting that the market for telehealth services would reach more than $130 billion worldwide by 2025," said Jackson. "It was recently projected that the U.S. market is expected to reach $10 billion by the end of this year, and experienced an 80% growth rate due to COVID-19."

Pandemic Accelerates Telehealth Trend

Telehealth visits in March 2020 surged by 50% as the pandemic took hold, and virtual health care interactions are on pace to top 1 billion visits in 2020, Jackson said. He laid out four major types of telehealth:

- **Mobile health platforms.** Mobile health is a general term for the use of mobile and other wireless technologies in medical care.
- **Real-time interactive services.** These, which encompass true "telemedicine" services, include such areas as telestroke, telepsychiatry and teleradiology services; continuous medical education; and teleconsultation.
- **Store-and-forward services.** This part of telehealth collects clinical information, such as demographics, medical history, laboratory reports, images, and sound and video files, and sends them electronically to another location for evaluation. It's most common in radiology, pathology, dermatology and ophthalmology.
- **Remote patient monitoring**. This is used for a variety of conditions, including diabetes, heart disease,

dementia, substance abuse, infertility and weight gain/loss.

"Clearly the emphasis right now is on video conferencing technology, but you've also got telerehabilitation where you oversee the rehabilitation of patients, which is facilitated by real-time interactions and clinical assessments," Jackson said. "These telerehabilitation sessions can be carried out via webcams, live chats or video conferencing platforms. There's telenursing, where nurses can use real-time interaction and the telemedicine platform to check on patient progress, monitor symptoms and make sure their condition isn't worsening."

Telepharmacy—consultations with pharmacists—along with teledermatology and teleophthalmology also are increasing in popularity, he said.

Attack Vectors Should Sound Familiar

Security threats to telehealth vary depending on the type of service involved, but generally speaking, all telehealth is vulnerable to security breaches simply because of its dependence on devices, Jackson said. Common threats include:

- Phishing attacks
- Ransomware and advance persistent threats
- Loss or theft of equipment
- Accidental or intentional data loss
- Attacks against connected medical devices

"We have to remember that what we're dealing with is a system where we're in a network of networks, and we're extremely interconnected," Jackson said. "So when we take a look at vulnerabilities, you have to look at telehealth systems as being part of the Internet-of-Things almost by definition because of their heavy reliance on internet and communications technologies. That interconnectedness is what makes them so useful but also so vulnerable."

The Open Web Application Security Project (OWASP), a nonprofit foundation that works to improve the security of software, publishes a top ten list of Internet-of-Things vulnerabilities:

- Weak, guessable or hardcoded passwords
- Insecure network services
- Insecure ecosystem interfaces
- Lack of secure update mechanisms
- Use of insecure or outdated components
- Insufficient privacy protection
- Insecure data transfer and storage
- Lack of device management
- Insecure default settings

- Lack of physical hardening

"Keep in mind that, when we're dealing with telehealth, we're dealing with three systems almost simultaneously," he said. "You're dealing with the vendor and the platform, you're dealing with the provider's environment and you're also dealing with the patient environment. So pretty much anything that you look at as far as a risk or vulnerability, you have to triple [the risk] because those threats and vulnerabilities exist in three interconnected arenas."

For example, many of the OWASP vulnerabilities come into play in a patient's home during a telemedicine visit, including weak passwords, outdated antivirus software and the use of insecure, outdated components, Jackson said. "You could be using a router that's way past its end-of-service and not even be aware of insufficient privacy protection." Families share devices and passwords, which also can be an issue, and many households feature insecure default settings and a lack of physical hardening for their devices, he said.

"All of this points to the need for having secure deployment of telehealth systems," he said.[2]

Contact Jackson via Clearwater spokesperson Skye McIntyre-Bolen at skye@growwithfuoco.com.

1 George Jackson, "Security Considerations for Deploying Telehealth & Remote Patient Monitoring Systems," Clearwater webinar, April 24, 2020, https://bit.ly/3b1x8Ql.
2 Jane Anderson, "Telehealth/Telemedicine Security Checklist," *Report on Patient Privacy* 20, no. 5 (May 2020).