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.