Report on Patient Privacy Volume 21, Number 6. June 10, 2021
Risks Multiplying With Expanded Telehealth, Telemedicine Services

By Jane Anderson

Telehealth and telemedicine applications have boomed during the COVID-19 pandemic, creating opportunities for providers and patients to connect more efficiently and effectively, yet potentially opening wide security vulnerabilities that cybercriminals can exploit.

George Jackson Jr., senior principal consultant at Clearwater Compliance LLC, a cyber risk management firm based in Nashville, explained how to identify and manage telehealth security risks during a recent webinar.[1]

“We know that telehealth and telemedicine adoption has surged over the past couple of years,” Jackson said. “A recent report said that 56% of U.S. consumers have used telemedicine and telehealth alternatives, especially during the pandemic, which was a jump of 11% since 2019.” In fact, it wasn’t clear prior to the pandemic that telehealth was going to take off, but “after the pandemic, there was no question left about it,” he said, adding that the U.S. telehealth market was valued at $10 billion in 2020 and is expected to reach $43 billion by 2026.

The growing adoption of telehealth expands the threat surface and raises cybersecurity concerns, Jackson said. Fifty-seven percent of patients recently surveyed said they believe virtual tools used by health care providers have increased the risk of their personal health information being compromised. Meanwhile, he added, nearly one-third of established digital health businesses rate the threat of cyberattacks or system failures as their number one business risk. “All the practical, empirical evidence seems to bear that out,” Jackson said.

Telehealth systems often involve a platform that features several environments, Jackson said. There’s the end-user environment, the intermediary environment—that’s typically the cloud—and the health delivery organization environment. There may also be a vendor environment before or after the provider, he noted.