Report on Patient Privacy Volume 21, Number 4. April 08, 2021 As Pandemic Enters 2nd Year, CISOs Face Ongoing Telework, Telemedicine Challenges

By Jane Anderson

As the COVID-19 pandemic progressed from its urgent beginning to almost a "new normal," chief information security officers (CISOs) at health systems have been fighting to combat emerging cyberthreats while supporting the sudden shift to telemedicine and working from home. In doing so, the officers said, the experience offers lessons for the path forward.

Five privacy and cybersecurity experts offered their take on the pandemic and what it revealed about the health care industry's cyber strengths and weaknesses on March 22 at the 30th annual National HIPAA Summit, which was held virtually.[1]

"Last March was a pretty big blur," said Jacki Monson, vice president and chief privacy and information security officer at Sutter Health in northern California. "Literally from one day to the next, we went from having a couple of hundred workforce members working from home to close to 15,000." This affected security, of course, but it also affected workflow, she said. "Things are different with people working in the office versus at home, and there's lots of security issues and lots of privacy issues that we had to accommodate."

Telemedicine was a major, urgent issue, Monson said. Prior to the pandemic, Sutter Health had some telemedicine activity, but when California canceled all inpatient and outpatient appointments in March, the health system had to move as many appointments as possible to telemedicine, she said. "We went from about 400 or 500 telemedicine visits to close to 200,000 a day within a couple of weeks when the pandemic hit, and there's all kinds of challenges and opportunities that came with that with respect to security."

HHS helped by issuing emergency public health exceptions that allowed providers some flexibility with telemedicine early in the pandemic, Monson said. But the health system still had to select and implement telemedicine platforms, all while the pandemic was building, she said. At the same time, "we also saw the cybersecurity numbers of potential attacks triple. And so it was just a very, very busy time trying to manage it all."

Monson said that her team did not experience any furloughs. However, many workforce members in field offices, hospitals and clinics did, "because obviously, when you close operations other than inpatient critical functions, you have a lot of workforce members that you just don't have work for." Bad actors seemed to realize this dynamic existed, she said. "We actually had some individuals approached at one of our affiliates to sell their user name and password for around $20,000 to give [the bad actor] multifactor authentication access to our systems." There also were issues surrounding access to COVID-19 research data, she said. "So I'm not sure we could have run with a smaller staff, and we have been very fortunate not to have been impacted by any layoffs or furloughs, just because of the criticality of the function. And we really believe that privacy and security is a patient safety issue, and so that's how my senior leaders contemplate needing to continue to invest in it."