COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 5. May 07, 2020 Telehealth/Telemedicine Security Checklist

By Jane Anderson

Health care organizations that already have telehealth programs—or those that have implemented them in response to the COVID-19 pandemic—should start off with a cyber-risk assessment for telehealth,[1] said George Jackson Jr., senior principal consultant at health care cyber-risk management firm Clearwater.

Assess risk for each information system that bears electronic protected health information (ePHI) "within your telehealth networking infrastructure and data storage system, ensuring there are no gaps," Jackson said. "You want to understand what risks you're exposed to, what risk are involved with your telehealth assets, and then assess what the highest risks are based on likelihood and impact."

Once an organization's telehealth and telemedicine risks have been assessed, the organization will need to implement risk response and remediation, with the goal of reducing residual risk as much as possible, he said. "On top of all that, you have to continue to assess and respond to the ever-evolving threat landscape through ongoing risk analysis and risk management."

There are six steps organizations can take to improve the security of their telehealth systems, Jackson said.

1) Establish a strong governance program. This includes creating a leadership committee, a business strategy and financial management for telehealth. It also includes ongoing training for staff; strong telehealth service planning, architecture and operations; and effective vendor, telehealth security and risk management.