Report on Patient Privacy Volume 19, Number 9. September 10, 2019 Checklist for Telehealth and Mobile Health Privacy, Security

By Jane Anderson

Properly safeguarding telehealth and mobile health programs and assets involves identifying all critical assets, applying appropriate controls and training, implementing detection mechanisms and continuous monitoring, and responding to and communicating about issues as they arise.

All of this needs to take place in a data-rich environment, according to George Jackson, Jr. with Clearwater Compliance LLC (see "Provider Organizations Should Take Lead on Complex Telehealth, Mobile Health Security," RPP 19, no. 9). "There is high value to this data," Jackson said. "It's a mouthwatering environment for hackers."

Jackson said that before beginning this work, security personnel at health care provider organizations need to ask themselves this question: "How solid is my cybersecurity foundation before I start adding on additional layers of risk?"