COSMOS
Navigate the Compliance Universe

# Report on Patient Privacy Volume 19, Number 9. September 10, 2019 Provider Organizations Should Take Lead on Complex Telehealth, Mobile Health Security

By Jane Anderson

Telehealth and mobile health technologies, two of the fastest-growing technologies in the health space, pose significant privacy and security challenges that organizations need to address. Doing so is likely to involve a complex, step-by-step incremental process that will span from vendors to patients, with provider organizations in control in the middle.

That's the word from George Jackson, Jr., a senior principal consultant with Clearwater Compliance LLC, who spoke recently at a webinar presented for members of the College of Healthcare Information Management Executives.

"Probably the biggest challenge in my opinion boils down to communications [between vendors, provider groups and patients], because there are so many moving parts," Jackson said. The health care delivery organizations providing telehealth and mobile health services need to understand the privacy and security threats and vulnerabilities, and the steps to mitigate those potential threats and vulnerabilities, he said.

Telehealth and mobile health together encompass monitoring, patient-to-provider and provider-to-provider chat, diagnostic services, remote testing (such as an EKG), remote treatment and other services. Hospitals and provider groups are investing in these technologies as insurers agree to reimburse for them.

For example, some 76% of hospitals reported in 2017 that they have fully or partially implemented a computerized telehealth system. Meanwhile, the Centers for Medicare and Medicaid Services last year finalized three new billing codes for remote patient services, including one that allows reimbursement for nonphysicians to remotely monitor patients who are chronically ill or who are recovering at home.