

Telemedicine, data security expected to grow in 2016

By [Joseph Conn](#) | January 1, 2016 - Modern Healthcare.com

2016 will be a year in which [telehealth](#) service delivery increasingly becomes central to the healthcare industry.

It's also likely there will be significant changes in the meaningful-use rules for electronic health records, and a beefing up of the long under-resourced area of [healthcare data security](#), experts say.

Technology watchers envision rapid acceleration in the adoption of telehealth services to address the needs of patients and providers as health systems increasingly are paid through value-based models.

“2016 is the time for telehealth,” said Nathaniel Lactman, a partner at Foley & Lardner who specializes in telehealth. A major factor, he said, is that providers are taking on more financial risk for managing the health of enrolled populations. “What a provider can do on the front end is use telehealth to make the patient more likely to interact with a clinician,” he said.

More states are allowing physicians to provide telehealth services across state lines through collaborative licensure arrangements. Meanwhile, 29 states and the District of Columbia have laws requiring health insurers to cover telehealth visits; similar laws are pending in six more states, Lactman said. Some insurers are moving on their own to cover telehealth services because they see them as cost-effective.

On [meaningful use](#), HHS in October released two rules for the \$31.7 billion EHR initiative, tweaking the federal regulations for the Stage 2 program, which is underway and establishing final rules for Stage 3, scheduled to start in 2017.

But Stage 3, as proposed, so poorly aligns with the new Medicare physician payment program Congress approved last spring that the Stage 3 program will need to be revised, said Dr. John Halamka, chief information officer of Beth Israel Deaconess Medical Center in Boston. Either HHS, which kept the “final” Stage 3 rules open for public comment, or Congress, which has several health information technology bills pending, will make the changes.

“I have optimism that there is going to be a delay in Stage 3 or a roll up” of Stage 3 into the new Medicare payment system, Halamka said.

The new year also is likely to bring more cyberattacks on healthcare data and higher spending on cybersecurity. “You can look forward to more hacking. We're not even close to slowing down,” said Michael McMillan, CEO of CynergisTek, an Austin, Texas-based data security consulting firm.

Fear of breach costs and damage to reputation is driving board-level scrutiny of security policies at many healthcare organizations. And with medical devices increasingly wired into patient data systems, “there is the potential (of hackers) to impact clinical care,” said Lucy Stribley, a senior vice president at security consultant Booz Allen Hamilton.

Many experts hope 2016 will be a year in which patients gain greater access to health data and tools to enable them to play a bigger role in managing their own health. Many healthcare organizations are struggling with how to increase members' use of their websites' patient information portals.

“We (should) get away from information tools being the sole purview of doctors and hospitals and give them to the American public,” said Dr. William Bria, executive vice president of medical informatics at the College of Healthcare Information Management Executives.