Report on Medicare Compliance Volume 28, Number 15. April 22, 2019

Medical-Device Security Has More Hurdles; 'Zero Trust' Is Option

By Nina Youngstrom

When HHS identified the top five cybersecurity risks faced by the health care industry in a December 2018 report, connected medical devices were right up there. Like other risks in the report, including phishing and ransomware, connected medical devices have the potential to expose all patient, billing and demographic information on hospital networks to hackers and other cybercriminals. Unlike the other risk areas, connected medical devices put hospitals in an exasperating position because often security measures are out of their hands, a consultant says. Medical device manufacturers have control over them and may resist prompt security updates, partly because they worry their devices will be adversely affected. That's increasing hospitals' vulnerability to cyberattacks, although they may be able to improve the security of their devices, including MRI and CT machines, by using measures that don't "touch" the machines.

"You have to go through the device manufacturer" for security updates, says Barry Mathis, consulting principal with PYA in Knoxville and a former hospital chief technology officer. "That's not something you have domain over. The device manufacturer has to be involved." It's frustrating for hospitals, which may be told by manufacturers they need Food and Drug Administration (FDA) approval for changes to improve cybersecurity, which he says isn't true (see box, p. 5).