COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 31, Number 18. May 16, 2022 'Ecosystem' of Connected Devices Heightens Cybersecurity Risk

By Nina Youngstrom

In a version of the future that hopefully never comes, malware is able to remove malignant-looking tumors from CT or MRI scans before they were reviewed by radiologists. The malware, which was part of an ethical hacking study by Israeli researchers, tricked three radiologists into misdiagnosing conditions virtually every time.[1] These types of attacks may be facilitated in part by insecure code that's prevalent in connected health devices. For example, an MRI machine typically has seven million lines of code, and programmers make, on average, 10 to 50 errors for every 1,000 lines of code.

"The errors in the code create vulnerabilities in the software that hackers and cybercriminals can then use to facilitate a cyberattack," said attorney Bethany Corbin, with Nixon Gwilt. "That's a lot of vulnerability to take into account when creating a cybersecurity strategy." It's one example of how connected health devices pose a risk to patients and the organizations that treat them, raising the stakes for mitigation strategies, including endpoint security and vendor audits, she said at a May 9 webinar sponsored by the Health Care Compliance Association.[2]

Connected health devices facilitate communication across platforms and the internet, enabling the transfer of data through a wireless infrastructure, she explained. Connected medical devices, also called the Internet of Medical Things (IoMT), are a subset of connected health.

10 to 15 Connected Devices Per Bed

There are two aspects of connected medical devices. One is the devices themselves. Some are implantable, such as wireless pacemakers or insulin pumps that are calibrated to the appropriate dosage, collect data from the patient and transfer it to the provider, Corbin said. The other aspect is the connected health system. "We are seeing the development of an ecosystem of devices under one roof," Corbin said. Connected hospitals have X-ray machines, MRIs and other connected devices, an estimated 10 to 15 connected devices per bed, according to American Hospital Association data cited by the Association for the Advancement of Medical Instrumentation.[3] "The area is seeing rapid growth, and most organizations are not well equipped to handle it from a privacy and cybersecurity perspective," she said.

The anticipated growth in connected health devices flows from their significant benefits, Corbin said. For one thing, "connected devices in health care have immense opportunity to benefit patients and providers by transforming the landscape of telehealth and enabling remote monitoring. Providers can establish constant connection with patients that allows physicians to monitor acute and chronic conditions without limiting patient mobility," she said.

There are also benefits in terms of behavioral modification and patient outcomes. "Connected health can encourage patients to take much more ownership of their conditions, especially chronic conditions," Corbin said. But the benefits must be weighed against the risks of harm, including jeopardizing privacy and security. For one thing, "health care data is highly sought after on the black market," Corbin said. Medical records can be sold for $250 apiece, far more than credit card and other financial data. While credit cards can be canceled, there's a

“perceived sense of permanence” with health data that make it very attractive to cybercriminals.

Also, connected medical devices can be a gateway to larger networks. For example, if a hospital has a bring-your-own-device policy, and there’s a vulnerability in the patient’s device, it can be exploited by hackers to enter the hospital’s network.

Another risk is legacy medical devices, because they “can’t be reasonably protected against current cyber threats,” Corbin said. “That creates a large threat surface that hackers can exploit. They’re already responsible for hospital cyberattacks.” These older devices weren’t built with cybersecurity attacks in mind, and “health care organizations have a significant number of legacy devices in their networks that are not monitored.”

The supply chain also exacerbates risks. “The product development ecosystem is becoming increasingly layered and complex, and that can allow the threat landscape to evolve,” Corbin said. “When health care organizations don’t know which components are in their software, it’s impossible to know about their vulnerabilities.”

Hackers who take over connected medical devices pose a risk to patient safety. Ethical hackers who test the systems have been able to take control of insulin pumps and dispense an entire reservoir of insulin as well as remotely install malware on pacemakers, Corbin said. “The loss of life is a particular risk, especially with implantable devices,” she said.