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.

Seven Mitigation Strategies for Connected Devices

Corbin recommended several mitigation strategies from a security perspective:

1. Endpoint security. Connected devices, such as smart IV pumps and inhalers, are known as endpoints because they can be used to access a hospital's IT framework. "You have to make sure connected devices are secure because hackers will try to access the larger network through endpoint devices." Corbin noted that IV pumps are one of the riskiest interconnected devices; 73% of them have a vulnerability that can jeopardize the security of the hospital's network. "Some people recommend having data secured by the cloud before it goes into the IT system to minimize the risk of it serving as a gateway to the entire system," Corbin said.

2. Vulnerability disclosure programs. This is a "structured form of ethical hacking to allow organizations to identify and mitigate risks," she said. Some organizations hire hackers (or sponsor competitions) to find vulnerabilities in their network security systems that might be exploited by malicious hackers. Vulnerabilities can be fixed before malicious hackers exploit them.

3. A software bill of materials. Like a food label, a software bill of materials is a list of device components, some of which are manufactured by unidentified third parties. "Right now, companies don't know what is contained in products because there's not a lot of visibility or transparency," Corbin said. Greater transparency would allow for identification and remediation of vulnerabilities. "If a vulnerability is identified in XYZ software, you could see if you have XYZ software in your device so you can patch it." President Biden's May 2021 cybersecurity executive order recommended a software bill of materials.[4]

4. Access and authentication controls. "Not every employee needs to have access to all the data," Corbin said. "When implementing data controls, think through what category of employees needs access to data sets to perform their job functions."

5. Network segmentation. Because every connected health device can serve as a gateway to a larger health care network that has possibly thousands of devices, hospitals should consider segmenting devices from the main network, Corbin said. "If devices are segmented, a breach related to devices won't spread to the

broader network, and you will have an easier time containing the breach."

6. Replacing and securing legacy devices. "Legacy equipment can't be updated to protect against newer cyber threats," Corbin noted.

7. Vendor audits. Hospitals have to ensure they properly vet vendors so they aren't "hacker stepping-stones if they fail to meet cybersecurity standards," Corbin said. "When hiring vendors, ensure their cybersecurity practices are disclosed and meet industry standards and that the contract guarantees you audit rights." She suggested focusing on high-risk vendors if there are too many to audit.

Supreme Court Decision Could Affect Certain Data

Corbin mentioned that she has received questions about the ripple effects of the leaked Supreme Court decision overturning Roe vs. Wade, the 1973 Supreme Court decision protecting a woman's right to have an abortion based on the right to privacy in the 14th amendment's due process clause. "I don't think HIPAA is at risk, because it's a federal law protecting data," she said. And the leaked decision "has been very clear that its rationale doesn't extend beyond abortion. But even if it doesn't threaten the fundamental right to privacy, there is a lot that can happen to connected health devices. We see a much greater threat landscape from that perspective."

There's a market called "female health technology," which includes apps and devices that collect sensitive data related to women's health. The market focuses on menstruation, ovulation, fertility, maternal health and other aspects of reproductive health. "Cyber criminals can see that as a new opportunity to come in and target femtech apps that are relatively new and may not have necessary cyber protocols and standards and get access to reproductive data and hold it for ransom," Corbin said. "If hackers reidentify the individual data, and it relates to abortions, they may extort individuals with the threat they will turn it over to law enforcement" in states that ban abortion.

Contact Corbin at bethany.corbin@nixongwiltlaw.com.

1 Rebecca Pifer, "Hackers manipulate lung cancer scans, fool radiologists and AI software in study," MedTech Dive, April 4, 2019, https://bit.ly/3Mglwwy.
2 Bethany Corbin and Ashleigh Giovannini, "Privacy and Security for Connected Health: The Good, The Bad and The Futuristic," webinar, Health Care Compliance Association, May 9, 2022.
3 Greg Garcia, "Connected Health and Cybersecurity: Advice about the Device," Association for the Advancement of Medical Instrumentation, November 17, 2021 https://bit.ly/3wGTuUr.
4 Improving the Nation's Cybersecurity, Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021), https://bit.ly/3hoPj9a.