COSMOS
Navigate the Compliance Universe

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).

"The FDA doesn't test devices for cybersecurity before they go into circulation," he notes. "The FDA approves them based on manufacturer testing. Some people say manufacturers can't update the device, but yes, they can—they don't want to. It's not the FDA saying the medical device manufacturer can't update the software." It's challenging for manufacturers as well because they have to ensure the anti-malware software and other security measures don't interfere with the medical device's function and reliability, Mathis explains.

Devices are a Conduit to Networks

Medical devices are vulnerable to hacking and other direct forms of cyberattacks, and they make hospitals vulnerable generally because they're increasingly connected to hospital networks, sending results to electronic health records (EHRs) for clinical, billing and other purposes. That includes X-ray machines, fetal monitors, blood-pressure cuffs, ultrasounds and even stethoscopes, to name a few. As a result, anyone with access to the medical device could access patient information. "It may be one patient or every patient seen that day or all patients over a period of time," Mathis says. The medical device also becomes a conduit to the other areas of the hospital network that are more vulnerable, he explains. "That single card at the bottom can bring down the house of cards" (see box, p. 6)

To protect medical devices from hackers and other cybersecurity threats, they require anti-malware software, patches, updates and other cybercriminal deflectors. "There are specific things medical device manufacturers have to do to guarantee to the FDA and the Department of Homeland Security that software can't be hacked, touched or manipulated," Mathis says. That's where two myths come in. First, people tend to think only the FDA is responsible for oversight of medical-device security, but "it's also the Department of Homeland Security" (DHS). Second, hospitals may think cybersecurity software updates (e.g., anti-virus, patches) apply universally,

but that's not the case. When they update software, hospitals are unable to apply it to most medical devices, Mathis says. "You can't go up to the device on your network and say, 'We will load Norton on all our machines.' If you do it, you will be violating your contract with the medical device company and breaking the support agreement," he says. "You have to go through the device manufacturers."

Suppose Java has an update, and it releases a note saying the current version is vulnerable to attack. Hospitals run an update, but they're not allowed to touch the medical devices. "They have to call the manufacturer, which says to wait until it releases the next version of the medical device," Mathis says. "Hospitals are forced to run an old, vulnerable version on their network." That jeopardizes the network, but there are physicians who insist on using the device anyway. By not updating Java, hospitals have increased the risk to their entire network and to the data on the device, he says.

Some medical device companies will tell hospitals their hands are tied because the medical device has only been approved by FDA with the original cybersecurity software, Mathis contends. But as the FDA itself states, it "does not typically need to review changes made to medical devices solely to strengthen cybersecurity." He notes that medical-device manufacturers are getting better about this; "they're on board with making sure cybersecurity is a priority, but they still insist you can't go out there and do anything and they have to be involved and it can slow down this process." Also, a lot of software updates are now built into medical devices, so the problems he's describing apply more to "legacy" devices. But security updates are still in the hands of device makers, not hospitals.

An Option: Making Devices Invisible

It's possible to sidestep these challenges by protecting the devices without touching them at all, Mathis says. "One of the ways I manage that vulnerability is with zero trust," he says. The concept of zero trust has been around since 2010, and it's becoming the norm for protecting devices, Mathis says. As the name implies, zero trust technology prevents everyone from connecting to a device in the network unless a person has specifically been given permission through authentication. "The device is seeing fewer people. I have already determined based on who someone is who can access the room," Mathis explains.

For fighting cybercrime, he thinks the most promising version of zero trust is the concept of first-packet recognition. It makes access to the data inside the medical device invisible to everyone except the users who have been identified as trusted. First-packet authentication doesn't require a device to acknowledge another device through the standard "handshake," Mathis explains. His analogy for first-packet recognition is a street with hundreds of houses where one house is completely invisible to everyone except the people who are allowed to see the door. "Imagine that in a hospital network," Mathis says. As far as hackers can tell, there are no medical devices because they've been cloaked. "I make it hidden from the rest of the world. You can use this technology to protect EHRs and even create a micro segmentation framework to protect many devices and systems." Mathis is only aware of one company, BlackRidge Technologies, that has patents for first-packet recognition, but other companies provide zero-trust technology.

Contact Mathis at bmathis@pyapc.com. View the December HHS cybersecurity report at http://bit.ly/2GlSGtH.