Health Information Compliance Alert

Medical Devices: Feds Warn Medical Devices Need Tighter Controls

Case uncovers cardiac implants vulnerable to cyber attack.

In a new report, **U.S. Department of Health and Human Services Office of Inspector General** (OIG) encourages more cyber protections for medical devices. Interestingly, a new case shows just how easy this technology is to infiltrate.

Details: The June release of the OIG's Semiannual Report to Congress for the first half of the 2019 fiscal year - October 1, 2018 to March 31, 2019 - covers the federal watchdog's efforts to rein in fraud and abuse in federal healthcare programs. In one of its biggest agency rebukes, OIG advises the **Food and Drug Administration** (FDA) that it's dropped the ball on medical device cybersecurity as well as incident response when medical devices do get hacked.

"FDA's policies and procedures were insufficient for handling postmarket medical device cybersecurity events," the OIG report maintains. "FDA had not adequately tested its ability to respond to emergencies resulting from cybersecurity events in medical devices; and, in 2 of 19 district offices, FDA had not established written standard operating procedures to address recalls of medical devices vulnerable to cyber threats."

The FDA admits that more needs to be done, especially in the wake of the rise of cyber attacks, the brief suggests. FDA agrees with OIG and plans to put these suggestions into practice:

- Assess its strategies for combating cyber threats.
- Work in step with the **U.S. Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team** to plan ahead.
- Establish stronger recall policies for vulnerable devices.
- Improve the FDA management of cybersecurity.

Take This Case in Point

If you are of the opinion that medical devices need to be encrypted, then you are in good company. Over the last year, **Medtronic Inc.,** the world's top medical device producer, has run into some trouble with some of its offerings. According to the FDA, they are easily compromised by cyber thugs.

Now: Some Medtronic "MiniMed insulin pumps are being recalled due to potential cybersecurity risks and [the FDA] recommends that patients using these models switch their insulin pump to models that are better equipped to protect against these potential risks," cautions a June 27 FDA release.

"While we are not aware of patients who may have been harmed by this particular cybersecurity vulnerability, the risk of patient harm if such a vulnerability were left unaddressed is significant," warns **Suzanne Schwartz, MD, MBA,** deputy director of the **Office of Strategic Partnerships and Technology Innovation** and acting division director for **All Hazards Response, Science and Strategic Partnerships** in the **FDA's Center for Devices and Radiological Health.**

See the MiniMed insulin pump information at www.fda.gov/news-events/press-announcements/fda-warns-patients-and-health-care-providers-about-potential-cybersecurity-concerns-certain.

Other issue: But this isn't Medtronic's first issue with worrisome medical device vulnerabilities. **DHS's Cybersecurity and Infrastructure Security Agency** warned in a March Medical Advisory that many of the manufacturer's "implanted cardiac defibrillators use an unencrypted wireless program that could allow computer hackers to change the settings," explains attorney **Jennifer Weed,** of Pennsylvania law firm **Gross McGinley LLP,** in a blog post.

CPT® 2023 American Medical Association. All rights reserved.

The product uses Conexus wireless telemetry protocol, according to the FDA. This causes the cardiac defibrillator to have "cybersecurity vulnerabilities because it does not use encryption, authentication, or authorization," a release says.

Important: Though DHS maintains no unauthorized access has been attempted on the cardiac defibrillators, it would be easy to technically hijack them as long as the hackers were close by. In fact, "the FDA confirmed that these vulnerabilities, if exploited, could allow an unauthorized individual (for example, someone other than the patient's physician) to access and potentially manipulate an implantable device, home monitor, or clinic programmer," says a release on the issue.

Find the cardiac defibrillator details at www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home.

Reminder: Wireless medical devices are an important part of medicine today, offering safer, more informed options that improve the delivery of care. But technology isn't perfect, and medical devices are ramping up to be the next big target for cyber criminals. "The FDA reminds patients, patient caregivers, and healthcare providers that any medical device connected to a communications network (for example: wi-fi, public or home Internet) may have cybersecurity vulnerabilities that could be exploited by unauthorized users," informs a March FDA release.

Resource: Review the OIG release at https://oig.hhs.gov/reports-and-publications/archives/semiannual/2019/2019-spring-sar.pdf.

CPT® 2023 American Medical Association. All rights reserved.