Bloomberg
BNA

Medical Devices Law
& Industry Report™

Safety

FDA Warns Manufacturers and Providers: Medical Devices Vulnerable to Cyberattack

The Food and Drug Administration June 13 issued an alert and draft guidance on medical device cybersecurity.

The agency said embedded computer systems in devices are vulnerable to cybersecurity breaches. FDA recommended that device manufacturers consider addressing cybersecurity measures for their products in premarket submissions.

The draft guidance, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, was announced in a notice published in the June 14 *Federal Register* (78 Fed. Reg. 35,940).

> **“The need for effective cybersecurity to assure medical device functionality has become more important with the increasing use of wireless, internet- and network-connected devices and the frequent electronic exchange of medical device-related health information,” FDA says.**

“The need for effective cybersecurity to assure medical device functionality has become more important with the increasing use of wireless, internet- and network-connected devices and the frequent electronic exchange of medical device-related health information,” FDA said in the notice.

The guidance, when finalized, will represent FDA’s “current thinking on management of cybersecurity in medical devices,” the agency said.

FDA, in the alert, recommended that medical device manufacturers “take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack.”

A medical device industry organization, the Advanced Medical Technology Association (AdvaMed), issued a statement in support of the draft guidance and safety alert.

“Despite the fact that there has been no patient harm as the result of either inadvertent or intentional cyber security breaches, we understand FDA’s desire to be cautious in this area,” Janet Trunzo, senior executive vice president of technology and regulatory affairs for AdvaMed, said in a release. “Patient safety is the number one priority of the medical technology industry, and manufacturers have in place numerous safeguards to ensure the security and integrity of their devices. The ubiquity of digital technologies offers patients significant benefits, and the risk of a malicious cyberattack is low when compared to these benefits.”

The FDA alert is intended for medical device manufacturers, hospitals, medical device user facilities, health care information technology and procurement staff, and biomedical engineers.

Comments on the draft guidance are due Sept. 12 (using docket FDA-2013–D-0616).

Attacks on Devices. Health care facilities, such as hospitals, should also take steps to evaluate their electronic medical record and device networks for possible security vulnerabilities, FDA said in the notice.

Any network-connected medical device, could be vulnerable to cyberattack, the agency said.

Cybersecurity experts have warned that the health care sector could become the focus of cyberattacks designed to steal personal information or harm patients.

FDA said it is not aware of any patient injuries or deaths associated with cyberattacks on medical devices. The agency will work closely with other federal agencies and device manufacturers to identify and mitigate security vulnerabilities.

Draft Guidance. The draft guidance provides recommendations on cybersecurity management measures for manufacturers preparing premarket submissions for medical devices.

The guidance document applies to all submissions for devices that contain software or programmable logic, FDA said.

FDA, in the guidance, recommended limiting access to medical devices capable of connecting to the internet or another network or device through a user authentication process. Manufacturers should use a multi-factor authentication process and automatically timed log-offs to ensure access is limited to trusted users, according to the draft guidance.

FDA recommended that medical manufacturers provide justification in their premarket submissions for the security features they choose.

Device manufacturers have already begun to take steps to reduce the risk of malicious cyberattacks, AdvaMed’s Trunzo said. This includes building device security into new product development processes and risk assessments, she said.

Documentation for Submissions. FDA also recommended that manufacturers submit documentation outlining the cybersecurity features of their devices.

This documentation should include:

- a hazard analysis and design consideration for cybersecurity risks associated with the device;
- a traceability matrix that links the cybersecurity controls of the device with risks considered;
- a plan for providing software updates for the device;
- a notice that the device will be provided to purchasers and users free of malware; and
- instructions for use of and specifications for antivirus software.

The agency's alert, or safety communication, noted that FDA has guidance in place ''on how manufacturers should address cybersecurity issues related to products that use off-the-shelf software.'' That guidance dates from 2005 (3 MELR 770, 11/18/09).

Attorney's Perspective. Attorney Greg Levine, with Ropes & Gray LLP, told BNA June 21 that although ''this is not the first time FDA has addressed cybersecurity and medical devices, it is the certainly the most concerted effort the agency has made and the first time FDA has made such specific recommendations.''

With FDA having increased awareness of this issue, Levine said he expects that device manufacturers ''will be hearing increasingly pointed questions from customers or potential customers on software security. One lesson from the FDA guidance is that manufacturers that haven't already done so should incorporate cybersecurity considerations into their design control procedures.''

In addition, Levine said that manufacturers that have older devices in the field should consider evaluating those devices to determine whether there are any additional measures they should take to enhance the security of those devices. ''This could require software patches or other modifications in some cases.''

Device manufacturers should also consider whether they have taken appropriate measures to ensure that their device software protects patient information, according to Levine. He added, ''Although that is not an FDA issue per se, the security of device software can affect both device performance as well as patient privacy. The device performance and privacy issues will be inextricably linked in many cases.''

Levine is a partner and co-chair of the Life Sciences Group at Ropes & Gray in Washington.

By Alex Ruoff

The notice in the ***Federal Register*** *is at http://www.gpo.gov/fdsys/pkg/FR-2013-06-14/html/2013-14167.htm.*

The draft guidance is at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.

The safety alert is at http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm.