HealthManagement
Promoting Management and Leadership

FDA Moves to Strengthen Cybersecurity of Medical Devices

The US Food and Drug Administration (FDA) has announced a new guidance for medical device manufacturers with regard to managing cybersecurity risks to better protect patient health and information. The federal agency noted that some medical devices and computer systems can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the devices.

The FDA's new guidance, titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," recommends that manufacturers consider cybersecurity risks as part of the design and development of a medical device, and that they submit documentation to the FDA about the risks identified and controls in place to mitigate those risks. Manufacturers also have to submit their plans for providing patches and updates to operating systems and medical software.

By carefully considering possible cybersecurity risks while designing medical devices and having a plan to manage system or software updates, manufacturers can reduce the vulnerability in their medical devices, the FDA said.

Medical devices are increasingly becoming more interconnected and interoperable. Thus, it is necessary for medical device developers to remain vigilant about cybersecurity and to properly protect patients from those risks, said Suzanne Schwartz, MD, MBA, director of emergency preparedness/operations and medical countermeasures at the FDA’s Center for Devices and Radiological Health. “There is no such thing as a threat-proof medical device."

The FDA is concerned about device-related cybersecurity vulnerabilities and their potential to adversely impact public health. The FDA’s concerns about cybersecurity risks include the following:

- Malware infections on network-connected medical devices or computers, smartphones, and tablets used to access patient data;
- Unsecured or uncontrolled distribution of passwords;
- Failure to provide timely security software updates and patches to medical devices and networks; and
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorised access to the device or network.

The agency did not provide any indication that specific devices or systems had been purposely targeted. It also did not say if any patients had been harmed as a result of cybersecurity breaches.

The FDA said it has been working closely with other federal agencies and the medical device industry to identify and communicate with stakeholders about vulnerabilities. It plans to hold a public workshop this fall to discuss how government, hospitals, medical device manufacturers, cybersecurity professionals, and other stakeholders can collaborate to improve the cybersecurity of medical devices and protect the public health.

The FDA is an agency within the US Department of Health and Human Services. Its duty is to protect the public health by assuring the safety, effectiveness, and security of human and veterinary drugs, vaccines and other biological products for human use, and medical devices. The FDA also is responsible for the safety and security of the country's food supply, dietary supplements, cosmetics, products that give off electronic radiation, and for regulating tobacco products.

Source: US Food and Drug Administration
Image Credit: Wikimedia Commons

Published on : Mon, 6 Oct 2014