HealthManagement
Promoting Management and Leadership

FDA Guidance for Mobile Devices

Amid criticism that it was not doing enough to address the cyber vulnerabilities in medical devices, the U.S. Food and Drug Administration has issued guidelines on how manufacturers can protect their products against cyberattacks. According to the guidelines, manufacturers must build cybersecurity controls into medical devices during the development process.

As part of risk management, manufacturers also will now be required to establish, document and maintain the identification of hazards throughout the device lifecycle.

The 30-page guidance was released as the FDA investigates reports that St. Jude Medical's heart devices are vulnerable to attacks that can endanger patient lives. Back in 2014, the FDA issued guidelines that addressed cybersecurity needs during new device development – but devices already available on the market were not covered.

See Also: **How Secure is the Healthcare Cloud?**

"Today's post-market guidance recognises today's reality: Cybersecurity threats are real, ever-present and continuously changing," said Suzanne B. Schwartz, MD, the FDA's associate director for science and strategic partnerships. "As hackers become more sophisticated, these cybersecurity risks will evolve."

The new document, however, does not include details on how the FDA would enforce these rules.

The FDA wants developers to apply the core rules of National Institute of Standards and Technology to improve cybersecurity infrastructure. In addition, manufacturers should assess vulnerabilities in their products and how they could affect patients, while working with researchers to better understand potential cyber risks.

Some in the healthcare industry have long criticised the FDA for only giving suggestions to fix these major security flaws – rather than offering official guidelines.

Issuance of the new guidance is part of the FDA's ongoing effort to address cybersecurity concerns, Schwartz said. "We'll continue to work with all medical device cybersecurity stakeholders to monitor, identify and address threats and intend to adjust our guidance or issue new guidance, as needed," she added.

Source: Healthcare IT News

Image Credit: Pixabay

Published on : Mon, 2 Jan 2017