Published on *The National Law Review* https://natlawreview.com

FDA Issues Final Guidance on Postmarket Cybersecurity

Article By:

Michele L. Buenafe

M. Elizabeth Bierman

Agency establishes a risk-based framework for assessment of postmarket cybersecurity risks for medical devices.

On December 28, 2016, FDA issued a final guidance titled "Postmarket Management of Cybersecurity in Medical Devices" (Final Guidance). A draft version of this guidance was issued in January 2016.

Medical devices, like other computer systems, are vulnerable to cybersecurity breaches, but breaches of medical devices can present significant public health risks as well as privacy and security concerns. FDA has taken a number of actions to help manage these risks, including issuance of guidance documents on premarket submissions for management of cybersecurity in devices,[1] issuance of safety communications on specific device cybersecurity vulnerabilities, and conduct of webinars and public workshops on cybersecurity issues. FDA has also entered into a Memorandum of Understanding with an Information Sharing Analysis Organization (ISAO), the National Health Information Sharing and Analysis Center, to help foster strategies to mitigate cybersecurity vulnerabilities and facilitate communication among various stakeholders.

FDA has encouraged device manufacturers to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, and maintenance of the device. The Final Guidance, however, focuses on postmarket management of such risks. In particular, it advises manufacturers on the applicability of FDA's medical device correction and removal reporting requirements (21 C.F.R. Part 806) to actions taken to address cybersecurity vulnerabilities.

The Final Guidance also is limited to actions taken by device manufacturers. FDA has not addressed actions taken by hospitals or other healthcare providers to manage cybersecurity vulnerabilities for the devices they use. However, given the criticality of cybersecurity to healthcare organizations and the increasing sophistication of hospital technology departments, these stakeholders may play a more significant role for medical device cybersecurity, as many hospitals and other healthcare organizations may be unwilling or unable to wait for device manufacturers to act, particularly for older devices that are no longer supported by the original manufacturer.

FDA's Risk-Based Model for Assessment of Medical Device Postmarket Cybersecurity Risks

The Final Guidance advises manufacturers to define and document their own process for assessing the cybersecurity risks for their devices, based on existing controls under their quality management plan. The main difference between the draft and final guidances relates to the criteria that manufacturers are advised to apply in assessing risk. Although the draft advised that manufacturers should assess the risk to a device's "essential clinical performance," the Final Guidance instead focuses on the risk of "patient harm," which correlates more closely to the Part 806 reporting requirements. The Final Guidance also includes a definition of "patient harm," which clarifies that loss of confidential information would not be considered "patient harm" for purposes of this guidance.

FDA recommends that manufacturers determine whether a risk to patient harm is controlled (i.e., acceptable) or uncontrolled (unacceptable). To make this determination, manufacturers are advised to use a matrix that looks at the exploitability of the cybersecurity vulnerability and the severity of patient harm if the vulnerability were to be exploited.

When vulnerabilities are determined to present a controlled risk, FDA generally does not intend to enforce reporting requirements under Part 806. This would include routine updates and patches that are made solely to strengthen cybersecurity or to address a vulnerability that could compromise personal health information. If manufacturers determine that a vulnerability presents an uncontrolled risk, the risks should be remediated promptly to reduce the risk of patient harm and reports should be filed with FDA as required by 21 C.F.R. Part 806.

However, even for vulnerabilities presenting uncontrolled risk, FDA does not intend to enforce Part 806 reporting requirements when

(1) there are no known serious adverse events or deaths associated with the vulnerability;

(2) the manufacturer communicates with its customers and user community regarding the vulnerability no later than 30 days of learning this information;

(3) the manufacturer fixes the vulnerability no later than 60 days after learning of it;

(4) the manufacturer actively participates as a member of an Information Sharing Analysis Organization (ISAO) that shares vulnerabilities and threats that impact devices and provides the ISAO with any customer communications upon notification of its customers[2];

(5) the remediation is included in any FDA-required annual reports; and

(6) device changes are assessed for pre-submission requirements (e.g., new 510(k)s).

Implications for Device Manufacturers

Device manufacturers will need to update their existing correction and removal reporting procedures to reflect the enforcement policy in this Final Guidance. Manufacturers also should ensure that they have adequate procedures for assessment and remediation of cybersecurity vulnerabilities of their medical devices.

[1] FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct. 2, 2014).

[2] The Final Guidance describes what constitutes “active participation.”

National Law Review, Volume VII, Number 10

Source URL:https://natlawreview.com/article/fda-issues-final-guidance-postmarket-cybersecurity