THE
NATIONAL LAW REVIEW

FDA Releases Draft Guidance on Postmarket Management of Cybersecurity in Medical Devices

McDermott Will & Emery
Article By
Vanessa K. Burrows
Jennifer S. Geetter
Daniel F. Gottlieb
Michael W. Ryan
McDermott Will & Emery
Publications - Insights

- Biotech, Food, Drug
- Communications, Media & Internet
- Health Law & Managed Care

- All Federal

Wednesday, January 27, 2016

On January 15, 2016, the ***U.S. Food and Drug Administration (FDA)*** published a draft guidance entitled *Postmarket Management of Cybersecurity in Medical Devices* (Draft Guidance), which outlines FDA's recommendations for managing postmarket cybersecurity vulnerabilities in medical devices that contain software or programmable logic and software that is a medical device, including networked medical devices. The Draft Guidance represents FDA's latest attempt to outline principles intended to enhance medical device cybersecurity throughout the product lifecycle.

Unlike other federal regulators, FDA primarily focuses on the cybersecurity risks to patient safety rather than on risks to personal information privacy and consumer protection. But, the Draft Guidance provides cybersecurity risk management recommendations that are generally consistent with those of other regulators and information security experts. For example, the FDA encourages manufacturers to follow the voluntary *Framework for Improving Critical Infrastructure Cybersecurity* developed by the National Institute of Standards and Technology with input from various government agencies and the private sector.

The Draft Guidance also comes shortly after the 2016 Work Plan release by the U.S. Department of Health and Human Services Office of Inspector General (OIG), which indicates that the OIG will examine whether FDA's oversight of hospitals' networked medical devices is sufficient to effectively protect associated electronic protected health information and ensure Medicare beneficiary safety. According to the OIG, its review will focus on dialysis machines, radiology systems, medication dispensing systems and other computerized medical devices that are integrated with electronic medical records and the larger health network. The cybersecurity efforts of multiple federal agencies sends a clear message that cybersecurity in health care will continue to be a priority for regulators in 2016.

The FDA requests that stakeholders submit comments on the Draft Guidance by April 21, 2016.

The following sections discuss the Draft Guidance's relationship to prior FDA cybersecurity guidance, its key recommendations and the implications for manufacturers as well as health information technology (IT) developers, health care providers and other stakeholders with responsibilities for medical device cybersecurity.

FDA's Premarket Cybersecurity Guidance

The Draft Guidance follows the FDA's release on October 2, 2014, of its final *Guidance for Premarket Submissions for Management of Cybersecurity in Medical Devices*, which offered recommendations to help manufacturers identify and consider issues relevant to cybersecurity risk management during the device design and development phase, as well as to prepare premarket submissions for such products. The Draft Guidance notes that manufacturers cannot mitigate cybersecurity risks through premarket controls alone. FDA emphasizes that manufacturers should monitor, identify and address cybersecurity vulnerabilities and successful exploits of vulnerabilities as part of their postmarket management of medical devices.

FDA Recommendations in Draft Guidance

Comprehensive Cybersecurity Risk Management Programs

Because cybersecurity risks to medical devices are continually evolving, the FDA believes it is "essential" that manufacturers implement ongoing comprehensive cybersecurity risk management programs as part of their compliance with the FDA's Quality Systems Regulation (QSR). The QSR sets forth requirements for the methods used in, and the facilities and controls used for, the design, manufacture, packaging, labeling, storage, installation and servicing of all finished medical devices intended for human use, including requirements for complaint handling, quality audits, corrective and preventive actions, software validation and risk analysis, and servicing. The QSR is intended to ensure that finished devices will be safe and effective and otherwise in compliance with the Federal Food, Drug, and Cosmetic Act (FDCA).

In general, cybersecurity risk management programs should address vulnerabilities that may impact patient safety and permit unauthorized access, modification, misuse, denial of use or unauthorized use of information. Critical components of such programs include:

- *Defining Essential Clinical Performance*. Defining “essential clinical performance” (*i.e.*, the performance that is necessary to achieve freedom from unacceptable clinical risk) in order to develop mitigations that protect, respond and recover from the cybersecurity risk
- *Identification*. Monitoring cybersecurity information sources to identify and detect cybersecurity vulnerabilities and risk
- *Intake and Handling Processes*. Establishing and communicating processes for vulnerability intake and handling
- *Risk Assessment*. Characterizing and assessing the exploitability and severity of detected vulnerabilities and risks
- *Disclosure Policy*. Adopting a coordinated vulnerability disclosure policy and practice
- *Mitigation and Response*. Responding to risks and vulnerabilities by deploying mitigations that address cybersecurity risk early and prior to exploitation

Defining Essential Clinical Performance

The Draft Guidance advises device manufacturers to define a device’s essential clinical performance; to identify the severity of different outcomes if the device is compromised; and to set forth risk acceptance criteria. According to the FDA, defining essential clinical performance will enable a device manufacturer to assess the impact of security vulnerabilities and triage such vulnerabilities for remediation.

Cybersecurity Information Sharing

As part of the identification component of a comprehensive cybersecurity risk management program, FDA encourages device manufacturers to participate in a cybersecurity Information Sharing Analysis Organization (ISAO) to facilitate sharing and dissemination of cybersecurity information and intelligence pertaining to vulnerabilities and threats across multiple sectors. Throughout the Draft Guidance, FDA emphasizes that cybersecurity is a shared responsibility with health care providers and other stakeholders.

Risk Assessment Process

FDA recommends that device manufacturers establish a defined, objective process to systematically evaluate risk and determine whether a cybersecurity vulnerability affecting a medical device presents an acceptable or unacceptable risk. FDA emphasizes that an analysis of the risks to a device’s essential clinical performance should include an assessment of both the exploitability of the cybersecurity vulnerability and the severity of health impact to patients if the vulnerability were exploited. To perform these assessments, the FDA recommends using a cybersecurity vulnerability assessment tool to rate vulnerabilities and determine the need for and urgency of the response (*e.g.,* the Common Vulnerability Scoring System) and the ANSI/AAMI/ISO 14971 standard (Application of Risk Management to Medical Devices) to assess the severity impact to health, if the cybersecurity vulnerability were to be exploited.

In all cases, FDA recommends that manufacturers make a binary determination that a vulnerability is either controlled or uncontrolled using an established process that is tailored to the product, its essential clinical performance, and the situation. A vulnerability is considered controlled when there is a sufficiently low residual risk that the device's essential clinical performance could be compromised by successful exploitation of the vulnerability. In contrast, a vulnerability is uncontrolled when there is unacceptable residual risk that the device's essential clinical performance could be compromised due to insufficient risk mitigation and compensating controls with respect to such vulnerability.

Risk mitigations, including compensating controls, should be implemented when necessary to bring the residual risk to an acceptable level.

Response to Controlled Risks/Vulnerabilities and Device Manufacturer Reporting Requirements

When a manufacturer determines that a vulnerability is controlled, the FDA recommends that it adopt the following changes or compensating controls:

- Routine updates and patches intended to increase device security and/or remediate vulnerabilities (but not to reduce a risk to health or correct a violation of the FDCA) and other changes to a device made solely to strengthen cybersecurity (which are typically considered "device enhancements" and generally do not trigger FDA reporting requirements under FDA's correction and removal reporting requirements); and

- For premarket approval devices with periodic reporting requirements, manufacturers should report newly acquired information concerning cybersecurity vulnerabilities and device changes made as part of cybersecurity routine updates and patches to FDA in a periodic (annual) report.

Response to Uncontrolled Risks/Vulnerabilities

For vulnerabilities determined to be uncontrolled risks, the FDA recommends the following changes or compensating control actions:

- Manufacturers should remediate the vulnerabilities to reduce the risk of compromise to essential clinical performance to an acceptable level;

- If it is not feasible or immediately practicable to implement a complete solution to remove a cybersecurity vulnerability from a medical device, manufacturers should identify and implement risk mitigations and compensating controls, such as a work-arounds or temporary fixes, to adequately mitigate the risk;

- Manufacturers should report these vulnerabilities to the FDA under the correction and removal reporting requirements, unless reported under another FDA reporting requirement. The FDA states, however, that it does not intend to enforce reporting requirements under the correction and removal requirement if:

- There are no known serious adverse events or deaths associated with the vulnerability;
- Within 30 days of learning of the vulnerability, the manufacturer identifies and implements device changes and/or compensating controls to bring the residual risk to an acceptable level and notifies users; and
- The manufacturer is a participating member of an ISAO.

- Remediation of devices with annual reporting requirements (*e.g.,* Class III devices) should be included in the annual report;
- Manufacturers should evaluate the device changes to assess the need to submit a premarket submission;
- Manufacturers should provide their customer base and user community (*e.g*., hospitals, physicians, patients) with relevant information on recommended work-arounds, temporary fixes and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions; and
- For premarket approval devices with periodic reporting requirements, information concerning cybersecurity vulnerabilities and the device changes and compensating controls implemented in response to this information should be reported to FDA in a periodic annual report.

If a device manufacturer does not take steps to remediate an uncontrolled risk that is essential to its clinical performance, the FDA may find a reasonable probability that use of, or exposure to, the device will cause serious adverse health consequences or death. The FDA will consider such devices to be in violation of the FDCA and subject to enforcement action.

Submitting Comments

Stakeholders that wish to submit comments to FDA should contact their regular McDermott lawyer or the authors of this newsletter. To ensure consideration of comments before the FDA begins working on the final version of the guidance, FDA recommends that stakeholders submit comments by April 21, 2016.

Source URL: https://www.natlawreview.com/article/fda-releases-draft-guidance-postmarket-management-cybersecurity-medical-devices