ROPES & GRAY ALERT

FDA Regulatory ▪ Digital Health

January 17, 2017

FDA Finalizes Guidance on Postmarket Management of Medical Device Cybersecurity

On December 28, 2016, the Food and Drug Administration (FDA) issued final guidance on the postmarket management of cybersecurity in medical devices.[1] The guidance outlines nonbinding recommendations on how device manufacturers should monitor, identify, and address cybersecurity vulnerabilities. It also describes a risk-based framework to help manufacturers determine when device modifications that address cybersecurity vulnerabilities must be reported to FDA.

Device manufacturers should review this final guidance and consider how to incorporate its recommendations into their postmarket management activities. This Alert summarizes key aspects of the guidance and identifies key differences from the draft version issued in January 2016.[2]

I. General Principles of a Postmarket Cybersecurity Management Program

The growing use of networked medical devices has opened important new avenues for improving patient care. At the same time, these developments have increased the exposure of devices and computer networks to cybersecurity threats. Failure to maintain cybersecurity can impact device functionality and result in patient harm, loss of data, or exposure of other connected devices to security threats.

To address cybersecurity vulnerabilities during the premarket development stage, FDA has previously recommended that manufacturers consider cybersecurity during the design and software validation process for a device. FDA's recommendations are outlined in its 2014 guidance, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," discussed in a previous Ropes & Gray Alert.

Recognizing that not all cybersecurity risks can be foreseen and mitigated solely through premarket activities, however, FDA considers it essential that manufacturers implement postmarket cybersecurity risk management programs. The final postmarket cybersecurity guidance recommends that a postmarket cybersecurity risk management program address vulnerabilities that may permit unauthorized access, modification, misuse, or denial of use of a device, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and that may result in patient harm. Specifically, FDA recommends that such a program include the following critical components:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risks;
- Maintaining robust software lifecycle processes that include mechanisms for monitoring third-party software components for new vulnerabilities and performing design validation and validation for software updates and patches used to remediate vulnerabilities;
- Understanding, assessing and detecting vulnerabilities;

[1] FDA Guidance, "Postmarket Management of Cybersecurity in Medical Devices" (Dec. 28, 2016).
[2] FDA Draft Guidance, "Postmarket Management of Cybersecurity in Medical Devices" (Jan. 15, 2016). *See* Ropes & Gray's previous Alert on the draft guidance.

- Establishing and communicating processes for cybersecurity vulnerability intake and handling;
- Using threat modeling to define how to maintain safety and essential performance of a device by developing mitigations that protect, respond, and recover from a cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

FDA's guidance recognizes that cybersecurity is a shared responsibility between public and private stakeholders, a principle set forth in Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience. FDA encourages device manufacturers to adopt the recommendations on cybersecurity set out in the voluntary "Framework for Improvement Critical Infrastructure Cybersecurity" published by the National Institute of Standards and Technology (NIST), with collective input from various government agencies and the private sector. FDA also encourages device manufacturers to look to standards, guidelines, best practices, and frameworks established by the security industry to adopt a culture of cybersecurity risk management. In addition, FDA specifically encourages device manufacturers to share cybersecurity threat information as active participants in Information Sharing Analysis Organizations (ISAOs) and to be aware of sources of cybersecurity threat information that fall outside their typical information sources, such as the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

II. Cybersecurity Risk Management

FDA recommends that a manufacturer establish, document, and maintain throughout the lifecycle of a device an ongoing process for identifying cybersecurity hazards, estimating and evaluating the associated risks, controlling those risks, and monitoring the effectiveness of the controls. FDA believes that this process should include risk analysis, risk evaluation, risk control, and incorporation of production and post-production information. In evaluating the risk of patient harm, FDA recommends that manufacturers take into account the exploitability of the cybersecurity vulnerability and the severity of patient harm if the vulnerability were to be exploited.

The guidance also encourages manufacturers to define, as part of their comprehensive cybersecurity risk management program, the safety and essential performance characteristics of their devices, the resulting severity of patient harm if the cybersecurity of the device is compromised, and associated risk acceptance criteria. FDA defines "patient harm" to be physical injury or damage to the health of patients. FDA emphasizes threat modeling as a tool to facilitate the understanding and assessment of the vulnerability and the potential for patient harm. Threat modeling also helps determine whether a proposed remediation can be expected to control a risk of patient harm, such that the risk is an acceptable one. FDA recommends that manufacturers consider employing a cybersecurity vulnerability assessment tool or similar scoring system for assessing vulnerabilities and determining the need for, and urgency of, the response. FDA identifies one such tool in the guidance, the Common Vulnerability Scoring System, Version 3.0, as well as a number of additional standards and guidelines that may help triage vulnerabilities.

III. Remediating and Reporting Cybersecurity Vulnerabilities

Using the risk management tools and processes described above, FDA advises manufacturers to reach a binary determination on whether a particular risk is controlled or uncontrolled. If the risk is uncontrolled, FDA recommends implementing additional remediation measures until the risk is controlled. In the guidance, FDA encourages manufacturers to engage in efficient, timely, and ongoing assessment of cybersecurity risks in marketed devices. For routine cybersecurity software updates and patches, FDA states that it will not typically require premarket review to clear or approve the software changes. In addition, when a manufacturer strengthens a device's cybersecurity to address controlled risks of patient harm (i.e., where there is already sufficiently low residual risk of patient harm to the vulnerability), FDA considers those changes to be device "enhancements," as opposed to device "corrections." As a result, such changes are not required to be reported as device corrections under 21 C.F.R. Part 806. FDA also

states that changes to a device made solely to address loss of confidentiality of patient information are typically device enhancements that would not be required to be reported under 21 C.F.R. Part 806.

In contrast, when a manufacturer takes action to remediate an otherwise *uncontrolled* risk of patient harm (i.e., where there is unacceptable residual risk of patient harm due in the absence of additional risk mitigations), FDA states that a manufacturer should evaluate the device changes to assess the need to submit a premarket submission to the FDA (e.g., premarket approval application (PMA) supplement or a 510(k)). FDA explains that, in the absence of remediation, a device with uncontrolled risk of patient harm may be considered in violation of the Federal Food, Drug, and Cosmetic Act and be subject to enforcement action.

In addition, FDA states that remediations of uncontrolled risks would ordinarily be required to be reported to the agency as removals or corrections under 21 C.F.R. Part 806. However, through the guidance, FDA explains that it is establishing an enforcement discretion policy whereby FDA does not intend to enforce reporting requirements under 21 C.F.R. Part 806 for changes to address uncontrolled risks under certain circumstances. Specifically, FDA will not enforce reporting requirements if:

i. There are no known serious adverse events or deaths associated with the vulnerability;

ii. Within 30 days of learning of the vulnerability, the manufacturer notifies users of the vulnerability and identifies and implements a device change to bring the residual risk to an acceptable level;

iii. No later than 60 days after learning of the vulnerability, the manufacturer validates, implements, and distributes the deployable fix to its customers; and

iv. The manufacturer is an active participating member of an Information Sharing Analysis Organization (ISAO).

Device manufacturers should consider whether to modify their procedures for correction and removal reporting under 21 C.F.R. Part 806 to reflect this FDA policy.

FDA also explains that, for both controlled and uncontrolled risks, a manufacturer's changes to address those should be submitted in a periodic report to FDA if the device is approved under a PMA.[3]

IV. Criteria for Defining Active Participation by a Manufacturer in an ISAO

As noted above, one of the criteria for FDA's enforcement discretion policy on the reportability of non-routine cybsecurity-related device changes is whether the manufacturer is an active participating member of an ISAO. The final guidance lays out criteria for what it means to be an active participating ISAO member. Specifically, FDA says that it will consider whether:

- The manufacturer is a member of an ISAO that shares vulnerabilities and threats that impact medical devices;
- The ISAO has documented policies pertaining to participant agreements, business processes, operating procedures, and privacy protections;
- The manufacturer shares vulnerability information with the ISAO, including any customer communications pertaining to cybersecurity vulnerabilities; and

[3] *See* 21 C.F.R. § 814.84.

- The manufacturer has documented processes for assessing and responding to vulnerability and threat intelligence information received from the ISAO.

FDA recommends that manufacturers maintain objective evidence to demonstrate that their participation in an ISAO meets these criteria. FDA also notes that the agency's Center for Devices and Radiological Health has entered into a Memorandum of Understanding with one ISAO, the National Health Information Sharing & Analysis Center (NH-ISAC). FDA does not, however, take the position that manufacturers must participate in the NH-ISAC to meet the agency's criteria for ISAO participation.

V. Key Differences from Draft Guidance

The final guidance differs from the draft in several important respects. Among other things, the final guidance:

- Uses the potential for patient harm, rather than risk to the safety and effectiveness of the device itself, as the touchstone for assessing risks posed by cybersecurity vulnerabilities. This change focuses the guidance's risk management recommendations activities around risk to health, a concept with which device manufacturers are familiar from existing FDA regulations, rather than the new concept of "essential clinical performance" of a device that FDA had emphasized in the draft guidance.

- Extends to 60 days the time that device manufacturers have to remediate an uncontrolled risk while remaining subject to FDA's enforcement discretion policy for reporting a device correction under 21 C.F.R. Part 806, provided that the manufacturer communicates interim controls to its customers and the user community within 30 days after learning of the vulnerability. The draft guidance would have provided only 30 days to identify and implement device changes or controls to bring the risk to an acceptable level.

- Provides additional details and guidance to manufacturers on a number of subjects, including sources of guidance for performing risk management activities, the criteria for being considered an active participant in an ISAO, and additional examples of how to determine whether a risk is controlled or uncontrolled.

VI. Consequences for Medical Device Manufacturers

The increasing sophistication of software-driven and networked medical devices is delivering huge improvements in medical care, but also presents the potential for risks to patient health and privacy due to cybersecurity vulnerabilities. FDA's guidance document reflects the increasing expectations on device manufacturers to establish sophisticated, proactive cybersecurity practices and procedures that begin when a device is initially being designed and continue throughout the device lifecycle. Device manufacturers that have not already done so should consider conducting a comprehensive assessment of their cybersecurity practices and procedures, taking into account the recommendations in the FDA pre- and post-market guidance documents and third-party standards, and evaluate whether to become an active participant in an ISAO.

Ropes & Gray will continue to monitor developments in this area. If you have any questions, please contact any member of Ropes & Gray's FDA regulatory practice or your usual Ropes & Gray Advisor.