ROPES & GRAY ALERT

Digital Health ▪ FDA Regulatory

January 20, 2016

FDA Issues Draft Guidance on Postmarket Cybersecurity of Medical Devices

On January 15, 2016, the Food and Drug Administration ("FDA") released a draft guidance entitled, "Postmarket Management of Cybersecurity in Medical Devices," outlining recommendations that device manufacturers should implement to manage postmarket cybersecurity vulnerabilities. The draft guidance sets forth considerations for assessing and addressing postmarket cybersecurity vulnerabilities, which are continually evolving and not possible for device manufacturers to mitigate solely through premarket controls. The draft guidance also emphasizes that an effective cybersecurity risk management program should cover the premarket and postmarket lifecycle phases, and reminds industry of the recommendations set forth in FDA's 2014 guidance on "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," discussed in a previous Ropes & Gray Alert.

Device manufacturers should review this draft guidance document closely and consider its implications for the postmarket monitoring of their current products. The comment period will remain open for 90 days.

Government Initiatives to Address Cybersecurity Vulnerabilities

The cybersecurity postmarket draft guidance, together with the 2014 premarket guidance, are elements of a larger government initiative to strengthen the nation's cybersecurity systems. In February 2013, the President issued Executive Order 13636 and Presidential Policy Directive 21, which recognize that public and private stakeholders must enhance the cybersecurity and resilience of the nation's critical infrastructure, including within the healthcare and public health sector. Executive Order 13636 also called for the National Institute of Standards and Technology ("NIST") to develop a framework intended to reduce cybersecurity risks to critical infrastructure. The first version of the NIST's framework, released in February 2014, provides a structure that the draft guidance recommends device manufacturers use and adopt, outlining the elements of a cybersecurity risk management program (i.e., identify, protect, detect, respond, and recover). FDA's draft guidance incorporates several key principles of the NIST's framework, as described further below.

In addition, on February 13, 2015, the President issued Executive Order 13691, which encourages the development of Information Sharing Analysis Organizations (ISAOs) to serve as focal points for cybersecurity information sharing and collaboration within the private sector as well as between the private sector and the government. The draft guidance strongly recommends that device manufacturers voluntarily participate in an ISAO as part of a comprehensive proactive approach to managing postmarket cybersecurity threats and vulnerabilities, and to assuring the continued safety and effectiveness of marketed medical devices.

FDA's Recommendations on Postmarket Cybersecurity Management

The draft guidance outlines recommendations for the monitoring, identification, and remediation of postmarket cybersecurity vulnerabilities and exploits. According to the draft guidance, manufacturers' postmarket cybersecurity risk management programs should be implemented as part of the Quality System Regulation (21 C.F.R. Part 820), covering several QSR elements, including complaint handling (21 C.F.R. § 820.198), quality audit (21 C.F.R. § 820.22), corrective and preventive action (21 C.F.R. § 820.100), software validation and risk analysis (21 C.F.R. § 820.30(g)), and servicing (21 C.F.R. § 820.200).

I. Principles of a Postmarket Cybersecurity Management Program

According to the draft guidance, a postmarket cybersecurity risk management program should address vulnerabilities that may permit the 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 impact patient safety. The critical components of such a program should include:

- monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities;
- understanding, assessing, and detecting vulnerabilities;
- establishing processes for vulnerability intake and handling;
- defining essential clinical performance to develop mitigations that protect and recover from cybersecurity risks;
- adopting a coordinated vulnerability disclosure policy and practice; and
- deploying mitigations that address cybersecurity risks prior to exploitation.

II. Evaluation of Risk to Essential Clinical Performance

The draft guidance explains that not all cybersecurity vulnerabilities present patient safety concerns. Rather, medical device manufacturers should assess the impact of the vulnerability on the "essential clinical performance" of the device, defined as the performance necessary to achieve freedom from unacceptable clinical risk. The draft guidance recommends that device manufacturers define, as part of the postmarket cybersecurity risk management, the essential clinical performance of the device, the resulting severity outcomes if compromised, and the risk acceptance criteria. FDA also recommends that device manufacturers measure the risk to the device's essential clinical performance by considering (i) the exploitability of the cybersecurity vulnerability and (ii) the severity of the potential health impact.

III. Remediating and Reporting Cybersecurity Vulnerabilities

FDA encourages efficient, timely, and ongoing cybersecurity risk management for marketed devices. To this end, the draft guidance states that FDA will not typically require premarket review to clear or approve software updates and patches intended to improve cybersecurity. Similarly, the draft guidance states that changes to strengthen cybersecurity will typically be considered device enhancements that are not required to be reported as removals or corrections under 21 C.F.R. Part 806, unless the cybersecurity vulnerabilities may compromise the essential clinical performance of the device and present a reasonable probability of serious adverse health consequences or death. If the device is approved under a PMA, the manufacturer must submit periodic reports to FDA, which may include newly acquired information concerning cybersecurity vulnerabilities and device changes made as part of cybersecurity updates and patches.

The draft guidance also announces an enforcement discretion policy for changes or other actions to address uncontrolled risks to essential clinical performance. Under this policy, FDA does not intend to enforce reporting requirements under 21 C.F.R. Part 806 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 identifies and implements device changes and/or compensating controls to bring the residual risk to an acceptable level and notifies users, and (iii) the manufacturer is a participating member of an ISAO.

FDA explains that, in the absence of remediation, a device with uncontrolled risk to its essential clinical performance may be subject to mandatory recall or other agency action.

Consequences for Medical Device Manufacturers

Although FDA's cybersecurity efforts are relatively new, it is by now clear that this is an area of significant and increased FDA focus. Device manufacturers that have not already done so should be carefully assessing and

addressing potential cybersecurity vulnerabilities over the lifecycle of their devices. Manufacturers should exercise vigilance in monitoring postmarket cybersecurity information from all sources, assessing identified risks, and appropriately responding to vulnerabilities.

The release of FDA's draft guidance coincides with FDA's public workshop on January 20-21, 2016, to highlight past collaborative efforts, increase awareness of existing maturity models used to evaluate cybersecurity status, standards, and tools, and to identify unresolved gaps and challenges in the progress of medical device cybersecurity. Through the public workshop, FDA is seeking broad public input on strategies for addressing the medical device cybersecurity within the complex medical device ecosystem.

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.