Pepper Hamilton LLP
Attorneys at Law

FDA's Expanding Views on Cybersecurity and Medical Devices: Draft Guidance on Postmarket Management of Cybersecurity

CLIENT ALERT | February 2, 2016

Barry H. Boise | boiseb@pepperlaw.com
Christopher M. De Bono | debonoc@pepperlaw.com

MEDICAL DEVICE MANUFACTURERS NEED TO CONSIDER CYBERSECURITY CONTROLS IN ALL ASPECTS OF THE PRODUCT DEVELOPMENT PROCESS, FROM CONCEPTION THROUGH COMMERCIALIZATION.

In response to concerns about increased cybersecurity vulnerabilities, Congress and the Executive Office have recently taken steps to promote risk detection and encourage data sharing. Specifically, Congress broadly addressed permissive data sharing and related safe harbors through the Cybersecurity Information Sharing Act of 2015. This followed President Obama having issued an executive order on promoting private sector information sharing in February 2015. Cybersecurity has growing implications in

the mobile medical device space, and the Food and Drug Administration (FDA), for its part, issued guidance to manufacturers on the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (October 2, 2014), which incorporates the National Institute of Standards and Technology's proposed cybersecurity framework.[1]

On January 15, 2016, FDA expanded its cybersecurity focus to approved medical devices by issuing draft guidance on the Postmarket Management of Cybersecurity in Medical Devices. This guidance identifies steps manufacturers of networked medical devices should take to identify and address postmarket cybersecurity vulnerabilities that pose a risk to patient safety and public health. In addition, this guidance identifies which cybersecurity-related vulnerabilities and changes manufacturers must report to FDA and encourages the sharing of cybersecurity threat information as part of the postmarket surveillance process.[2]

A Plan for Cybersecurity Risk Management Will Be Needed

Recognizing that it is not possible to completely mitigate risks through premarket controls alone, FDA recommended that manufacturers promptly implement a cybersecurity risk management program to:

- Monitor cybersecurity information sources to identify and detect vulnerabilities and risks
- Detect, assess and understand the presence and impact of a vulnerability
- Establish and communicate processes for handling vulnerabilities
- Develop mitigation strategies to protect against, respond to and recover from risks
- Adopt a vulnerability disclosure policy and practice
- Develop preventive measures to mitigate and address risks early and prior to exploitation.

According to FDA, a key purpose of conducting the risk management assessment portion of this program is to determine whether cybersecurity vulnerabilities pose a risk to clinical performance that is "controlled" or "uncontrolled." A controlled risk is defined as

one where there is a sufficiently low residual risk that cybersecurity vulnerabilities could compromise the device's clinical performance, whereas an uncontrolled risk poses an unacceptable risk that performance could be compromised.

The judgment and classification of risk as "controlled" or "uncontrolled" is an important one. A manufacturer's reporting requirements under 21 C.R.F. 806.10 flow directly from this determination. FDA requires heightened reporting for uncontrolled risks. Specifically, FDA guidance would not require reporting of efforts taken "solely to strengthen cybersecurity" related to a controlled risk, but would require reporting actions taken in connection with an uncontrolled risk, if not already reported under 21 C.F.R. parts 803 or 1004.

FDA Creates Incentives to Notify Users and Participate in Information Sharing

FDA noted, however, that it does not intend to enforce the 21 C.F.R. part 806 reporting requirements for uncontrolled risk where the following conditions are met:

- The vulnerability does not result in serious adverse events or deaths
- The manufacturer notifies users of the risk and takes steps to bring it to an acceptable level within 30 days of learning of the vulnerability
- The manufacturer currently participates in an Information Sharing Analysis Organization (ISAO), such as NH-ISAC.

There is little direction, however, as to how this notification process would work. One possible example is how FDA issued its first cybersecurity alert to Hospira Inc., when an outside hacking threat posed a potential risk to patient safety with computerized infusion pumps designed for the continuous delivery of anesthetic or therapeutic drugs. An unauthorized user with malicious intent could access the pump remotely and modify the dosage it delivers. The safety communication was directed to hospitals with the particular system and provided specific guidance on how to mitigate against the threat.

FDA Would Impose Annual Reporting Requirements for Premarket Approval Devices

FDA also provided guidance on how manufacturers of premarket approval (PMA) devices should report cybersecurity risks, whether controlled or uncontrolled, as part of their

annual reporting requirements pursuant to 21 C.F.R. 814.84. FDA recommended that manufacturers include the following information in their annual reports:

- A description of the cybersecurity risk prompting the change and details on how the manufacturer learned of the vulnerability
- The conclusions of the manufacturer's risk assessment process and whether any identified risks were controlled or uncontrolled
- A description of any changes made to the device and the rationale for making them
- A list of all other devices that were modified in response to the same vulnerability
- The name of the ISAO to which the vulnerability was reported and the date of the report, if any
- References to any other relevant submissions (e.g., PMA supplement, 30-Day-Notice, 806 report) or the scientific or regulatory basis for concluding that a report was not required.

The overall message of this guidance is that medical device manufacturers need to consider cybersecurity controls in all aspects of the product development process, from conception through commercialization. There is a 90-day comment period for this draft guidance, and we will keep you posted on any further developments.

Endnotes

1. On October 2, 2014, FDA issued final guidance addressing premarket cybersecurity controls. *See Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, available at http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

2. For an analysis of FDA's guidance on premarket and design considerations, see our client alert "Unhack My Heart: FDA Issues Guidance to Mitigate Cybersecurity Threats in Medical Devices," available at http://www.pepperlaw.com/publications/unhack-my-heart-fda-issues-guidance-to-mitigate-cybersecurity-threats-in-medical-devices-2013-06-24/.