Cooley

FDA Issues Draft Cybersecurity Guidance to Medical Device Manufacturers

February 23, 2016

On January 22, 2016, the US Food and Drug Administration ("FDA") issued draft guidance outlining important steps medical device manufacturers should take to address cybersecurity risks in order to improve patient safety and better protect the public health. The draft guidance, entitled "**Postmarket Management of Cybersecurity in Medical Devices**" ("Draft Guidance"), details the agency's recommendations for monitoring, identifying and addressing cybersecurity vulnerabilities in medical devices once they have entered the market.

The Draft Guidance builds on a series of steps previously taken by the government to strengthen security of medical devices. In particular, the Draft Guidance builds on guidance regarding premarket cybersecurity concern previously issued in 2014 ("**Content of Premarket Submissions for Management of Cybersecurity in Medical Devices**" ("Premarket Guidance")) recommending that medical device manufacturers build safety controls into network-enabled devices in order to prevent the unauthorized access and theft of confidential medical information.

Key elements

In the Draft Guidance, the FDA advises medical device manufacturers to address security and privacy when designing and developing medical devices. This should be accomplished by creating design inputs for devices related to cybersecurity and establishing a cybersecurity vulnerability and management approach the company's risk analysis. The approach outlined in the Premarket Guidance provided that a device manufacturer's premarket approach should include the following elements:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies;
- Assessment of residual risk and risk acceptance criteria.

Although the Draft Guidance continues to stress that premarket controls should be addressed, the FDA notes that the cyber risks are continually evolving and therefore premarket controls can't alone address all potential risk. The Draft Guidance notes that device manufacturers must therefore implement a comprehensive risk management program consistent with the FDA's requirements contained in Quality System Regulation (21 CFR Part 820) including but not limited to complaint handling (21 CFR 820.198), quality audit (21 CFR 820.22), corrective and preventive action (21 CFR 820.100), software validation and risk analysis (21 CFR 820.30(g)) and servicing (21 CFR 820.200).

According to the Draft Guidance, a postmarket cybersecurity risk management program should apply the 2014 National Institute of Standards and Technology ("NIST") voluntary "**Framework for Improving Critical Infrastructure Cybersecurity**" to 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. Essential components of a cybersecurity risk management program should include:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

In order to manage these risks, medical device manufactures must establish methods to (i) "identify, characterize, and assess a cybersecurity vulnerability"; and (ii) "analyze, detect, and assess threat sources."

Evaluating risks of essential clinical performance

The FDA highlights the fact that not all cybersecurity vulnerabilities present patient safety concerns and recommends that device manufacturers define essential clinical performance for their products. Essential clinical performance means "performance that is necessary to achieve freedom from unacceptable clinical risk, as defined by the manufacturer." The Draft Guidance states that manufactures should consider the requirements necessary to achieve device safety and effectiveness. Risk to the device's essential clinical performance should be evaluated by considering (i) the exploitability of the cybersecurity vulnerability and (ii) the severity of the potential health impact.

Risk management and vulnerability assessment

A successful risk management program must be employed to identify, protect against, and respond to risks. The Draft Guidance suggests that the risks to a device's clinical performance should be evaluated by considering 1) the exploitability of the cybersecurity vulnerability; and 2) the severity of the health impact to patients if the vulnerability were to be exploited. The Draft Guidance outlines potential approaches and tools that can be used to assess such risks but notes that these risks will vary significantly depending on the device and uses.

Remediation and reporting

The Draft Guidance encourages "efficient, timely, and ongoing" risk management and remediation. The FDA notes that the majority of actions taken by device manufactures to address cybersecurity vulnerabilities and threats will be considered "cybersecurity routine updates or patches" for which the FDA does not require reporting under 21 CFR Part 806. However, for those cybersecurity vulnerabilities and threats that risk assessments determine may compromise the essential clinical performance of a device, notice will be required. The FDA notes that the purpose of conducting a risk assessment and determining what vulnerabilities exist is critical to determine whether the vulnerabilities identified are "controlled" (acceptable risk) or "uncontrolled" (unacceptable risk).

The Draft Guidance provides examples of the mitigation of controlled risks and uncontrolled risks. Uncontrolled risks are those where "there is an unacceptable residual risk that the device's essential clinical performance could be compromised due to insufficient compensating controls and risk mitigations."

The FDA outlines a discretionary policy of enforcement under which it does not intend to enforce reporting requirements under 21 CFR Part 806 for uncontrolled risks 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; and
- The manufacturer currently participates in an Information Sharing Analysis Organization ("ISAO").

The 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 CFR 814.84. The 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.

Incentives to notify users and participate in sharing of information

The Draft Guidance notes that sharing cyber risk information and intelligence within the medical device industry is critical to implementing a proactive approach to cybersecurity. Executive Order 13691-Promoting Private Sector Cybersecurity information Sharing (EO 13691), encourages the development of 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 FDA considers voluntary participation in an ISAO critical to managing cybersecurity threats. To that end, the FDA Centers for Devices and Radiological health has entered a Memorandum of Understanding with one such ISAO, the National Health Information Sharing & Analysis Center.

Practice tips

Medical device companies can take steps now to address this guidance by establishing a cybersecurity risk management program that includes the following elements:

- Identify
  - Define essential clinical performance
  - Identify cybersecurity signals
- Protect/Detect
  - Vulnerability characterization and assessment
  - Risk analysis and threat modeling
  - Analysis of threat sources
  - Incorporation of threat detection capabilities
  - Impact assessment on all devices
- Protect/Respond/Recover

- Compensating controls assessment
- Risk mitigation of essential clinical performance

Our **Health Care & Life Sciences** practice group works closely with our **Privacy & Data Protection** practice group to track these and other regulatory issues involving medical devices and cybersecurity. We can provide you with additional information or insights, tailored to your or your organization's needs.

The FDA encourages interested parties to respond to the Draft Guidance with comments. Public comments to the Draft Guidance should be submitted by April 21, 2016. Written comments may be submitted to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Electronic comments may be submitted to **www.regulations.gov**.

Please contact any of the contact attorneys on this client alert if you would like assistance submitting comments.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Vince Sampson Washington, DC	vsampson@cooley.com +1 202 728 7140
