Akin Gump
STRAUSS HAUER & FELD LLP

Medical Device Alert

January 28. 2016

Cybersecurity of Postmarket Medical Devices Addressed by FDA in Draft Guidance

If you read one thing

- FDA released Draft Guidance outlining steps for medical device manufacturers to ensure cybersecurity of medical devices already on the market; comments are due by April 21, 2016.
- The Draft Guidance encourages medical device manufacturers to develop procedures to identify, remediate and, in some cases, report cybersecurity vulnerabilities, based on how risks impact a device's "essential clinical performance."
- FDA proposed to waive certain reporting requirements for device sponsors that participate in an Information Sharing Analysis Organization.

The U.S. Food and Drug Administration (FDA or the "Agency") released much-awaited draft guidance on postmarket management of cybersecurity in medical devices ("Draft Guidance") on January 15, 2016,[1] just before the Agency's two-day public meeting on cybersecurity on January 20 and 21. The meeting agenda and webcast archive are available here. The Agency previously released Draft Guidance providing recommendations for addressing cybersecurity in medical devices in premarket submissions,[2] and industry eagerly awaited this companion Draft Guidance to address uncertainty regarding the responsibilities of medical device manufacturers with respect to medical devices already on the market.

Comments to the Draft Guidance, "Postmarket Management of Cybersecurity in Medical Devices," are due by April 21, 2016.[3]

---

[1] FDA, FDA *Outlines Cybersecurity Recommendations for Medical Device Manufacturers* (Jan. 15, 2016), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm; FDA, Draft Guidance for Industry and FDA Staff, Postmarket Management of Cybersecurity in Medical Devices (Jan. 22, 2016), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf [hereinafter "Draft Postmarket Guidance"].

[2] FDA, Draft Guidance for Industry and FDA Staff, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (June 14, 2013), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf [hereinafter "Draft Premarket Guidance"].

[3] 81 Fed. Reg. 3,803, 3,803 (Jan. 22, 2016), *available at* https://www.gpo.gov/fdsys/pkg/FR-2016-01-22/pdf/2016-01172.pdf.

Cybersecurity vulnerability is a growing concern as medical devices become more connected to the Internet, hospital networks and other medical devices.[4] These vulnerabilities may result in compromised device functionality, loss of medical or personal data integrity or availability, or exposure to other connected devices, which may adversely impact patient care. As one example, last year FDA issued a safety communication to health care facilities alerting them that Hospira's Symbiq Infusion System could be accessed remotely through a hospital's network, which would allow an unauthorized user to control the device and change dosage.[5] The pump has since been discontinued.

The new Draft Guidance applies to:

- medical devices that contain software (including firmware) or programmable logic
- software that is a medical device.

The Draft Guidance outlines (1) steps that manufacturers of medical devices should take to address cybersecurity risks continually by monitoring, identifying and addressing cybersecurity vulnerabilities in medical devices once they enter the market; and (2) associated requirements for reporting to the Agency.

Cybersecurity Management: Focus on "Essential Clinical Performance"

The Draft Guidance emphasizes that, even though manufacturers should implement controls when they are designing a product, this alone is insufficient to address cybersecurity risks. It is essential that manufacturers also implement comprehensive cybersecurity risk management programs and documentation consistent with FDA's Quality System Regulation[6] and respond to vulnerabilities in a timely manner. These programs should include:

- monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk
- understanding, assessing and detecting the 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

---

[4] Indeed, FDA released a Draft Guidance on the interoperability of medical devices on January 26. FDA, Draft Guidance for Industry and FDA Staff, Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices (Jan. 26, 2016), http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482649.pdf.

[5] FDA, Cybersecurity Vulnerabilities of the Hospira Symbiq Infusion System: FDA Safety Communication (July 31, 2015), http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm.

[6] Draft Postmarket Guidance, *supra* note 1, at 11; *see* 21 C.F.R. part 820.

- deploying mitigations that address cybersecurity risk early and prior to exploitation
- incorporating elements consistent with the National Institute of Standards and Technology Framework for Improving Cybersecurity Infrastructure Cybersecurity (i.e., Identify, Protect, Detect, Respond and Recover).[7]

The Draft Guidance also encourages medical device manufacturers to participate in an Information Sharing Analysis Organization (ISAO), a collaborative group that facilitates the sharing and dissemination of cybersecurity information among public and private sector members.[8] FDA has entered into a Memorandum of Understanding with one such ISAO, the National Health Information Sharing and Analysis Center (NH-ISAC).

The Agency's cybersecurity management framework centers on a new concept of "essential clinical performance," meaning "performance that is necessary to achieve freedom from unacceptable clinical risk, as defined by the manufacturer."[9] The degree to which a particular vulnerability impacts a device's essential clinical performance would determine the required remediation and reporting requirements, if any.

The Draft Guidance instructs manufacturers to consider requirements necessary to achieve device safety and effectiveness when defining the device's essential clinical performance.[10] Manufacturers should then design their risk management process to assess cybersecurity risk by considering:

- the exploitability of the cybersecurity vulnerability
- the severity of the health impact to patients if the vulnerability were to be exploited.

The Agency provides recommendations for assessing each of these factors[11] and describes how manufacturers should use that information to evaluate whether the risks to essential clinical performance are controlled (acceptable) or uncontrolled (unacceptable). These determinations dictate manufacturers' reporting obligations, as described below.

Reporting Requirements

Uncontrolled Risk to Essential Clinical Performance

According to the Draft Guidance, "uncontrolled risk" is present where there is unacceptable residual risk that the device's essential clinical performance could be compromised due to insufficient risk mitigations and external safeguards (known as "compensating controls").[12] The Agency instructs manufacturers to

---

[7] Draft Postmarket Guidance, *supra* note 1, at 11–2. The Draft Premarket Guidance recommends the adoption of these principles in product design. Draft Premarket Guidance, *supra* note 2, at 4.

[8] *Id*.

[9] *Id*. at 9.

[10] *Id*. at 13.

[11] *Id*. at 14.

[12] *Id*. at 18.

report these vulnerabilities under existing regulations that require reporting of certain actions concerning device corrections and removals (21 C.F.R. part 806, unless reported under 21 C.F.R. part 803 or 1004).[13] FDA will not, however, enforce reporting requirements if all of the following elements are met:

- there are no known serious adverse events or deaths associated with 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 within 30 days of learning of the vulnerability
- the manufacturer is a participating member of an ISAO, such as NH-ISAC.[14]

FDA notes that, without remediation, a device with uncontrolled risk to its essential clinical performance such that it presents a reasonable probability of serious adverse health consequences or death may cause the product to be in violation of the Food, Drug, and Cosmetic Act (FDCA) and subject to enforcement or other action.[15]

Controlled Risk to Essential Clinical Performance

FDA defines "controlled risk" as a sufficiently low level of residual risk that the device's essential clinical performance could be compromised by the vulnerability.[16] For example, a manufacturer may determine that a malware infection of the PC component of a medical device that collects browsing information, but does not impact the device's essential clinical performance, presents a "controlled risk."

In situations like this, the manufacturer may still update the product to strengthen cybersecurity, but the update would be considered a "cybersecurity routine update or patch," which would generally not require advance notification or reporting to the Agency under 21 C.F.R. part 806. Such "routine updates or patches" are defined as "updates or patches that increase device security and/or remediate vulnerabilities associated with controlled risk and do not reduce a risk to health or correct a violation of the [FDCA]."[17] A regularly scheduled security update, not performed to address a controlled risk, would also fall in this category. These routine updates would be considered device "enhancements," which typically do not carry reporting requirements. However, for devices that required premarket approval with periodic reporting requirements, newly acquired information concerning cybersecurity vulnerabilities and device changes made as part of routine update and patches should be reported to FDA in the device's periodic report.[18]

* * *

[13] *Id*. at 4; *see* 21 C.F.R. § 806.10 (providing requirements regarding reports of corrections and removals).
[14] Draft Postmarket Guidance, *supra* note 1, at 18.
[15] *Id*. at 19.
[16] *Id*. at 17.
[17] *Id*. at 8.
[18] *Id*. at 17.

Although the Draft Guidance does provide instructive information about the Agency's thinking on this topic, uncertainty remains as to how medical device manufacturers would implement the proposed requirements. FDA and stakeholders discussed these issues during FDA's workshop last week, where the Agency continued to encourage stakeholders to participate in a collaborative process to improve medical device cybersecurity.

Contact Information

If you have any questions regarding this alert, please contact:

Nathan A. Brown
nabrown@akingump.com
202.887.4245
Washington, D.C.

Christin Helms Carey
chcarey@akingump.com
202.887.4257
Washington, D.C.

Marlee P. Gallant
mgallant@akingump.com
202.887.4252
Washington, D.C.