Global Security Services | Cybersecurity
Health Law | Privacy, Data Security & Information Use
February 11, 2016

A Lifelong Commitment: FDA Releases Postmarket Guidance on Cybersecurity Risk Management for Medical Device Manufacturers

By Brian E. Finch, Gerry Hinkley, Kristi V. Kung and Caitlin Bloom Stulberg

On January 22, 2016, the Food and Drug Administration (FDA) issued draft guidance titled "Postmarket Management of Cybersecurity in Medical Devices," setting forth proposed recommendations for the medical device industry as well as FDA staff on the management of cybersecurity vulnerabilities in networked medical devices (such as insulin pumps, pacemakers and defibrillators) already in the marketplace.[1]

This Draft Guidance follows previously issued premarket guidance pertaining to cybersecurity vulnerabilities of medical devices, creating a regulatory scheme governing cyber threats throughout the devices' lifecycles. While the Draft Guidance does not establish legally enforceable responsibilities (i.e., nothing in the document should be considered binding or mandatory), it provides a potentially very interesting model for how manufacturers can categorize the risks posed by cyber-vulnerabilities in their medical devices, as well as when and how they might address those risks.

It also offers reduced reporting requirements under 21 C.F.R. Part 806 for manufacturers who voluntarily adopt the recommendations and join an Information Sharing Analysis Organization (ISAO). In particular, medical device manufacturers should take note of the FDA's comprehensive attention to the cybersecurity threats posed by networked medical devices as well as the risk management strategies for identifying and addressing cyber vulnerabilities.

[1] "Postmarket Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff," dated January 22, 2016.

Key takeaways from the Draft Guidance include:

- Implementation of Cybersecurity Risk Management Plans
- Controlled versus Uncontrolled Risks
- Cybersecurity Disclosure Requirements only for Vulnerabilities and Exploits that May Compromise the Essential Clinical Performance of a Device
- Impact of Involvement in an ISAO on Certain Reporting Requirements

Medical device manufacturers that may be affected by the Draft Guidance have until **April 21, 2016**, to submit comments. Written comments should be submitted to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852, and electronic comments should be submitted to http://www.regulations.gov.

A New Front in the Struggle for Cybersecurity

Attention to medical device cybersecurity by government agencies skyrocketed several years ago following reports about possible cyber-vulnerabilities in insulin pumps. As more medical devices began to incorporate wireless capabilities and network to hospitals, health systems, and other health care entities, the risks to both patient safety and protected health information intensified. These concerns were noted in President Obama's 2013 Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, which called for enhanced security, cybersecurity information sharing, and implementation of risk-based standards. Recent large-scale cyberattacks have continued to highlight cybersecurity concerns associated with medical devices connected to the Internet. With more Americans than ever now relying on the efficacy and safety of networked medical devices, many experts view medical device vulnerabilities as one of the key cybersecurity issues for 2016.

The Draft Guidance is the latest of several steps that the FDA has taken to address and manage the cybersecurity threats posed by the increasing number of medical devices that are vulnerable to cybersecurity threats (i.e., devices that incorporate software and are connected to an IT network, such as certain pacemakers, surgical robots and insulin pumps). In October 2014, the FDA issued guidance encouraging medical device manufacturers to consider cybersecurity threats during the design and development process (i.e., security by design) and describing how manufacturers should prepare premarket submissions for those devices.[2] The FDA's first device-specific action to combat cybersecurity risks followed on July 31, 2015.[3]

With the issuance of the Draft Guidance, which focuses on addressing postmarket cybersecurity threats, the FDA has made clear that the threat imposed by cybersecurity should be considered throughout the duration of a device's lifecycle. The Draft Guidance clarifies the FDA's postmarket recommendations related to cybersecurity in (i) medical devices that contain software or programmable logic and (ii) software that is a medical device.[4] In addition, the Draft Guidance emphasizes industry's role in monitoring,

[2] "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," dated October 2, 2014.
[3] "Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication," July 31, 2015.
[4] The Postmarket Draft Cyber Guidance does not apply to experimental or investigational medical devices.

identifying, and addressing cybersecurity vulnerabilities as part of the postmarket management of medical devices.

Interestingly, the FDA is on the path to developing cybersecurity guidance that is more realistic and flexible than typically seen out of federal regulatory agencies. More specifically, the Draft Guidance does not take a "one size fits all" approach to medical device cyber-vulnerabilities. Rather, as laid out in the Draft Guidance, in the majority of instances actions taken by manufacturers to address cybersecurity vulnerabilities and exploits will be considered "routine" and will not require advance notification or reporting under 21 C.F.R. Part 806.

However, for a small subset of cybersecurity vulnerabilities and exploits that may compromise the "essential clinical performance" of a device and present a reasonable probability of serious adverse health consequences or death, the FDA will require notification by the manufacturer. The Draft Guidance follows the FDA's midline approach to health IT, balancing risk without stifling innovation.

Cybersecurity Risk Management Program. According to the FDA, it is "essential" that manufacturers implement a structured and systematic comprehensive cybersecurity risk management program that would include the following components, among others:

- Application of the National Institute of Standards and Technology cybersecurity framework (including the core principles of "Identify, Protect, Detect, Respond and Recover");
- Monitoring of cybersecurity information sources to identify cyber risk;
- Assessment of the impact of known vulnerabilities;
- Adoption of a coordinated vulnerability disclosure policy; and
- Mitigation of cybersecurity threats prior to exploitation.

As part of a manufacturer's risk management process under 21 C.F.R. Part 820, the manufacturer should establish, document, and maintain throughout the medical device lifecycle an ongoing process for identifying hazards associated with the cybersecurity of the medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of such controls. Manufacturers should define and document their process for objectively assessing their cybersecurity risk, including risk analysis, risk evaluation, risk control, and incorporation of production and post-production information.

Risk Assessment for Essential Clinical Performance. In the Draft Guidance, the FDA emphasizes that a risk management process should focus on assessing a device's "essential clinical performance," a term newly created by the FDA. The FDA defines "essential clinical performance" to mean performance that is necessary to achieve freedom from unacceptable risk as defined by the manufacturer and describes that "[c]ompromise of the essential clinical performance can produce a hazardous situation that results in harm and/or may require intervention to prevent harm." Manufacturers can determine the risk to a device's essential clinical performance by considering: (i) the exploitability of the cybersecurity vulnerability, and (ii) the severity of the health impact to patients if the vulnerability were to be exploited.

To assess the exploitability of the cybersecurity vulnerability, the FDA recommends that manufacturers use a cybersecurity vulnerability assessment tool for rating vulnerabilities and determining the need for and urgency of the response. The FDA highlights as an example the "Common Vulnerability Scoring System,"

Version 3.0, which offers numerical ratings corresponding to high, medium and low. Likewise, manufacturers should have a process for determining the severity impact to a patient's health if cybersecurity vulnerability were to be exploited. The FDA acknowledges that there are many acceptable approaches for conducting this type of analysis, but highlights as an option the qualitative severity levels approach described in ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices – Application of Risk Management to Medical Devices.

A key purpose of conducting the risk assessment is to "evaluate whether the risk to essential clinical performance of the device is controlled (acceptable) or uncontrolled (unacceptable)." A vulnerability is deemed controlled when there is a sufficiently low (acceptable) residual risk that the device's essential clinical performance could be compromised by a cybersecurity vulnerability. Conversely, a vulnerability is deemed uncontrolled when there is an unacceptable residual risk that the device's essential clinical performance could be compromised due to insufficient compensating controls and risk mitigations.

Notification and Reporting Recommendations. The Draft Guidance clarifies that device manufacturers must notify the FDA regarding serious cybersecurity vulnerabilities and exploits, but not for issuing routine updates and patches to devices and software that are already on the market. Importantly, as an incentive for adopting the Draft Guidance, the FDA announced that device manufacturers who adopt these recommendations and join an ISAO will be relieved of certain uncontrolled risk reporting. Specifically, in cases where vulnerability is quickly addressed in a way that sufficiently reduces the risk of harm to patients or device users, the FDA does not intend to enforce urgent reporting of uncontrolled risks if:

- There are no serious adverse events or deaths associated with the vulnerability;
- Within 30 days of learning of the vulnerability, the manufacturer notifies users and implements changes that reduce the risk to an acceptable level; and
- The manufacturer is a participating member of an ISAO and reports the vulnerability, its assessment, and remediation to the ISAO.

In the absence of remediation, a device with uncontrolled risk to its essential clinical performance may be considered to have a reasonable probability that use of, or exposure to, the product will cause serious adverse health consequences or death and may be in violation of the Federal Food, Drug and Cosmetic Act (FD&C Act) and subject to enforcement. Further, for premarket approval devices with periodic (annual) reporting requirements, information concerning cybersecurity vulnerabilities, device changes and compensating controls implemented in response to this information should continue to be reported to FDA in a periodic (annual) report. The Draft Guidance provides examples of where notifications will and will not be required.

Information Sharing Analysis Organization. The FDA's recommendations in the Draft Guidance include promotion of information sharing through participation in an ISAO. The FDA urges the medical device and health IT community to participate in ISAOs to develop a shared understanding of the risks posed to networked medical devices by cybersecurity vulnerability and so that ISAO participants may identify, and take timely and appropriate action to mitigate the risks of such vulnerabilities. While voluntary, the FDA considers participation in an ISAO a "critical component" of a medical device manufacturer's comprehensive proactive approach to management of postmarket cybersecurity threats and vulnerabilities.

The Department of Health and Human Services Office of Inspector General's 2016 Work Plan includes review of the FDA's oversight of hospital's networked medical devices and whether such oversight is

sufficient to protect electronic protected health information (ePHI) and ensure beneficiary safety. Significant focus in the Work Plan is placed on the growing threat that networked medical devices have on a health system's electronic health record privacy and security. Thus, while the FDA's Draft Guidance focuses on the efficacy of the device and patient safety concerns, future attention will likely turn to vulnerabilities such devices pose to unauthorized disclosures and breaches of ePHI.

In addition to cybersecurity risk mitigation, Pillsbury has extensive experience with addressing the privacy and security of ePHI and responses to security incidents and breaches. Our Privacy, Data Security & Information Use focus team has been recognized by *Chambers Global* as one of the world's foremost privacy and information law practices.

If you have any questions about the content of this alert please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Brian E. Finch (bio)
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com

Gerry Hinkley (bio)
Los Angeles
+1.213.488.7188
gerry.hinkley@pillsburylaw.com

Kristi V. Kung (bio)
Washington, DC
+1.202.663.8037
kristi.kung@pillsburylaw.com

Caitlin Bloom Stulberg (bio)
San Francisco
+1.415.983.1023
caitlin.stulberg@pillsburylaw.com

Pillsbury Winthrop Shaw Pittman LLP is a leading international law firm with 18 offices around the world and a particular focus on the energy & natural resources, financial services, real estate & construction, and technology sectors. Recognized by *Financial Times* as one of the most innovative law firms, Pillsbury and its lawyers are highly regarded for their forward-thinking approach, their enthusiasm for collaborating across disciplines and their unsurpassed commercial awareness.