NOVEMBER 2014

COMMENTARY

FDA Voices Privacy Concerns and Promotes Medical Device Cybersecurity with New Guidance, Collaborative Information-Sharing

- FDA recently issued guidance on cybersecurity requirements for premarket submissions of medical devices and held a two-day workshop among policymakers, industry leaders, and security experts focused on promoting best practices in the health care and public health sector.
- In addition, FDA has partnered with the National Health ISAC to facilitate information-sharing and develop a cyber risk assessment framework and mitigation strategies for medical device manufacturers.

Cybersecurity of medical devices poses unique challenges for industry and regulators, because of potential risks in device malfunction, disruption of medical care, and compromised patient data, as well as the challenge of balancing countervailing needs, such as patient safety and ensuring that devices are readily accessible. Based on recent actions, the U.S. Food & Drug Administration ("FDA") appears committed to addressing these challenges.

Last month, FDA issued final guidance on "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" ("Premarket Cybersecurity Guidance").[1] The Premarket Cybersecurity Guidance outlines basic principles of cybersecurity and describes general controls for manufacturers to adopt and document during development of a medical device. The release of this document was followed by a two-day, multiagency workshop focused on the broader topic of cybersecurity in health care.

As FDA continues to engage in information-sharing about relevant threats and vulnerabilities, these ongoing efforts present opportunities for stakeholders to help develop a risk assessment framework customized for the health care device sector. Although FDA supports a collaborative, multisector approach to cybersecurity, the Premarket Cybersecurity Guidance clarifies that device manufacturers, rather than user facilities or software vendors, are responsible for ensuring software integrity, design maintenance, and appropriate cybersecurity controls.

FDA Cybersecurity Workshop: Jump-Starting the Dialogue

On October 21–22, 2014, in partnership with the U.S. Departments of Health and Human Services and Homeland Security, FDA hosted a public workshop on

"Collaborative Approaches for Medical Device and Healthcare Cybersecurity." The initiative, which coincided with National Cybersecurity Awareness Month, included representatives from medical devices manufacturers, health care providers, trade organizations, government agencies, and information security firms.

At the outset, FDA emphasized the goal was to promote an open, ongoing dialogue among stakeholders about current cyber threats, potential vulnerabilities, and industry best practices. Event organizers made clear this two-day workshop, consisting of 10 panels and four keynote speeches, would be a springboard for future initiatives on the topic. The following provides a brief summary of some key discussions:

- Panelists framed the problem by explaining current cyber threats, dissemination and communication practices, and related enforcement actions. There was broad consensus about the need for collaboration among public and private stakeholders in the health care sector.
- Discussions about cybersecurity gaps and challenges identified the following issues: the desire to balance security and usability issues during a device's development phase, rather than addressing these issues in a retrofit; the need to update a device's risk assessment throughout its lifecycle (which might exceed the labeled or expected life due to an operator's extended use); additional risks of networking devices and using off-the-shelf software; and confusion among manufacturers regarding FDA policy on software upgrades.
- White House Cybersecurity Coordinator Michael Daniel described the need for a holistic approach to cyber preparedness and prevention, accounting for technical needs (such as workforce development), business realities (by prioritizing and optimizing solutions to better manage risks), and human psychology (by making cybersecurity the default rule, rather than an opt-in feature). In February 2014, the National Institute of Standards and Technology ("NIST") issued a general framework for industry that outlines five core functions of cybersecurity activities: (i) identify cybersecurity risks to systems, assets, data, and capabilities, while understanding the business context; (ii) protect critical capabilities and services with appropriate safeguards; (iii) detect cybersecurity events in a timely manner; (iv) respond with appropriate action; and (v) recover capabilities and services impaired by cybersecurity events.[2]
- The panelists acknowledged that patient safety must be the primary focus during the development of cybersecurity tools and standards for the health care sector. Several panelists recommended looking to other industries, such as the financial sector, for ways to integrate consistent and effective security solutions. They also suggested modifying technical standards from other contexts, such as industrial controls, to medical devices. Industry must address primary vulnerabilities—choices in the design of systems that create cyber risks and errors in the actual coding or implementing of those systems—which requires involving everyone, from front-line providers and patient safety experts to IT personnel and security professionals.

Participants also explored possible "paths forward" on health data security. They acknowledged that regulation and voluntary efforts by individual companies and trade associations will continue and encouraged these stakeholders to keep communication channels open. Although the theme of the workshop was much broader than FDA's recent Premarket Cybersecurity Guidance, some panelists described the document as a positive step toward fostering security considerations at the earliest stages of device development, while acknowledging opportunity for more concrete standards.

New Guidance: Design Validation Requirements for Cybersecurity

FDA has yet to promulgate specific regulations on cybersecurity, instead opting to address its expectations in guidance documents that explain existing rules. The Premarket Cybersecurity Guidance applies to all premarket submissions for medical devices that are or contain software or programmable logic,[3] and it aims to encourage the adoption of basic security controls through the design validation process of the Quality System Regulation. In general, manufacturers must establish and follow reasonable procedures for validating that a device's design conforms to user needs and intended uses.[4] FDA has long included software validation as part of a finished device's design validation, which requires confirmation through simulated and user-site testing that the software can consistently fulfill the particular requirements of the device.[5]

This latest Premarket Cybersecurity Guidance extends these validation requirements to the area of cybersecurity, encouraging relevant risk assessments and design inputs at the earliest stages of device development. Endorsing the five core functions outlined by the NIST, the Premarket Cybersecurity Guidance encourages manufacturers to identify and assess the impact of threats and vulnerabilities on device functionality and patients, determine suitable mitigation strategies, and assess residual risk and risk acceptance criteria. More specifically, manufacturers should develop a set of cybersecurity controls and provide the following information in their premarket submissions:

- Hazard analysis, mitigations, and design considerations regarding intentional and unintentional cybersecurity risks, including lists of all risks considered in the design of the device and all controls adopted to mitigate such risks;
* A traceability matrix linking actual cybersecurity controls to the risks considered;
* A plan for providing validated software updates and patches as needed throughout the device's lifecycle;
* A summary describing controls in place to ensure the device software will maintain its integrity (e.g., remain free of malware) from the point of origin to the point at which that device leaves the manufacturer's control; and
* Instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g., anti-virus software, use of firewall).

The third item listed above—a plan for providing validated software updates and patches—reflects the reality that a device's security controls will evolve over the life of the device and may therefore require post-market validations. Many of these post-market adaptations, such as software patches, do not require FDA review, as long as they do not create a new or changed indication for use or significantly affect the safety or effectiveness of the device. However, any time a software change is made, the manufacturer is instructed to complete comprehensive validation testing to determine "the extent and impact of that change on the entire software system."[6] Another guidance document on cybersecurity reminds manufacturers to document such changes and the reasons supporting them in the design history files, and for devices approved under PMAs, to explain such changes in the annual report to FDA.[7]

Next Steps: Information Sharing, Framework Development

The Premarket Cybersecurity Guidance will unlikely be FDA's last word on the issue. During the workshop, participants were keen to note the long path to optimal security, some of which is already underway. In August 2014, FDA entered into a memorandum of understanding with the National Health Information Sharing & Analysis Center, Inc. ("NH-ISAC"), which contemplates a mutual sharing among FDA, NH-ISAC, and its member companies of information about cybersecurity vulnerabilities and threats in medical devices.[8] The parties intend to develop a shared risk assessment framework that will help stakeholders consistently and efficiently assess patient safety, public health, and health technology infrastructure risks and implement best practices.

As for the workshop, FDA plans to post a transcript of the discussions to its website. Interested parties are encouraged to submit public comments through November 24, 2014, via email to AskMedCyberWorkshop@fda.hhs.gov, or directly to Docket FDA-2014-N-1286. To facilitate the discussion, FDA provided the following questions:

- Are stakeholders aware of NIST's Cybersecurity Framework? If so, how might FDA adapt or translate the Framework to meet the medical device cybersecurity needs of the health care and public health sector?
- How can FDA establish partnerships within the health care sector to quickly identify, analyze, communicate, and mitigate cyber threats and medical device security vulnerabilities?
- How might the stakeholder community create incentives to encourage sharing information about medical device cyber threats and vulnerabilities?
- What lessons learned, case studies, and best practices (from within and external) might incentivize innovation in medical device cybersecurity in the health care and public health sector? What are the cybersecurity gaps from each stakeholder's perspective: knowledge, leadership, process, technology, risk management, or others?
- How do health care and public health stakeholders strike the balance between the need to share health information and the need to restrict access to it?

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Laurie A. Clarke
Washington
+1.202.879.3498
lclarke@jonesday.com

Colleen M. Heisey
Washington
+1.202.879.3449
cmheisey@jonesday.com

Kevin D. Lyles
Columbus
+1.614.281.3821
kdlyles@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Alexis S. Gilroy
Washington
+1.202.879.5552
agilroy@jonesday.com

Matthew R. Bowles
Washington
+1.202.879.3604
mbowles@jonesday.com

Endnotes

[1] U.S. Food & Drug Admin., "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff" (Oct. 2, 2014).

[2] Nat'l Inst. of Standards & Tech., "Framework for Improving Critical Infrastructure Cybersecurity" at 8-9 (2014).

[3] The guidance applies broadly to premarket approval applications, premarket 510(k) notifications (including traditional, special, and abbreviated), de novo submissions, Product Development Protocols, and Humanitarian Device Exemption submissions. FDA further advises that manufacturers may also consider these principles for Investigational Device Exemption submissions and devices exempt from premarket review. "Premarket Cybersecurity Guidance" at 2.

[4] 21 C.F.R. § 820.30(g).

[5] *See* U.S. Food & Drug Admin., "General Principles of Software Validation; Final Guidance for Industry and FDA Staff" at 6 (Jan. 11, 2002).

[6] *Id.* at 12; *see also* 21 C.F.R. § 820.30.

[7] U.S. Food & Drug Admin., "Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software" at 4; *see also* 21 C.F.R. § 820.30(j).

[8] MOU No. 225-14-0019 between Nat'l Health Info. Sharing & Analysis Ctr., Inc., and U.S. Food & Drug Admin., Ctr. for Devices & Radiological Health (Aug. 26, 2014).

Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.