FDA Final Guidance Confirms Role of Medical Device Firms in Cybersecurity Management

On October 2, 2014, the Food and Drug Administration ("FDA") released the final version of a guidance document entitled, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." As discussed in a previous Ropes & Gray Alert, the draft guidance released in June 2013 provided recommendations for the development and documentation of cybersecurity management in medical device premarket submissions. Although FDA made some organizational changes in the final guidance, the substance is similar to the draft. Device manufacturers should review this guidance document closely and consider its implications for the design of their current products as well as future premarket submissions.

Cybersecurity Vulnerabilities and Government Initiatives to Address Them

As detailed in Ropes & Gray's prior Alert, last year's draft guidance was accompanied by an FDA safety alert recommending that device manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of device failure due to cyberattack. Although FDA has not identified any specific instances of patient injuries or deaths associated with cybersecurity incidents, the agency noted that it was aware of specific cybersecurity vulnerabilities, such as the presence of malware on hospital computers and mobile devices and a lack of timely security updates and software patches (particularly for older devices).

FDA's final guidance for device manufacturers also follows on several government-wide orders and initiatives to strengthen cybersecurity. In February 2013, the President issued Executive Order 13636 and Presidential Policy Directive 21, which recognize that public and private stakeholders must enhance the cybersecurity and resilience of the nation's critical infrastructure, including the healthcare and public health sector. Executive Order 13636 also called for the National Institute of Standards and Technology ("NIST") to develop a framework intended to reduce cybersecurity risks to critical infrastructure. The initial version of the NIST's framework, released in February 2014, provides a structure that organizations can use to create, guide, assess, and improve comprehensive cybersecurity programs. FDA's final guidance incorporates several key principles of the NIST's framework, as noted further below.

FDA's Recommendations on Cybersecurity Management

The final guidance identifies cybersecurity-related issues that manufacturers "should consider in the design and development" of medical devices and in preparing premarketing submissions. Specifically, the guidance recommends that manufacturers establish cybersecurity-related design inputs and develop a cybersecurity vulnerability and management approach as part of the risk analysis required under 21 C.F.R. § 820.30(g) of the Quality System Regulation.

The final guidance describes a flexible approach with respect to the particular security controls that are appropriate for a particular device, taking into consideration, among other factors, the device's intended use, its intended environment of use, the type of cybersecurity vulnerabilities present and likelihood of exploitation, and the probable risk of patient harm due to a cybersecurity breach. While the examples of security controls described in the final guidance are essentially the same as those set forth in the final guidance, FDA has reorganized these controls based on the five "core" cybersecurity functions described in the NIST's framework: Identify, Protect, Detect, Respond, and Recover.

In response to the draft guidance, some device manufacturers and industry trade groups acknowledged that cybersecurity-related documentation should be included in device design history files, but argued that such information should not be required in premarket submissions. It is unclear, for example, how the inclusion of

such information would be relevant to the "substantial equivalence" standard for FDA clearance of a premarket notification submission under section 510(k) of the Federal Food, Drug, and Cosmetic Act. Nonetheless, FDA maintained its position in the final guidance that device premarket submissions should include cybersecurity-related information, including, among other things, a hazard analysis pertaining to cybersecurity risks, a traceability matrix linking specific cybersecurity risks to specific controls, and a plan for providing software updates and patches as needed throughout the lifecycle of the device.

Notably, the final guidance places less emphasis on confidentiality considerations than the draft guidance. Whereas the draft guidance stated that manufacturers should assure cybersecurity to maintain the "confidentiality, integrity, and availability" of medical device information, this statement was removed from the final guidance.[1] As finalized, the guidance contains a definition of "confidentiality," but the term is not used elsewhere in the document. This revision perhaps reflects FDA's recognition that confidentiality and patient privacy considerations are not a core FDA concern, but rather are addressed by privacy laws enforced by other agencies. For example, device manufacturers acting as business associates to entities covered by the Health Insurance Portability and Accountability Act (HIPAA), such as hospitals and physician offices, must comply with applicable requirements of the HIPAA Security and Privacy Rules and are subject to direct liability for any violations of such rules.

Consequences for Medical Device Manufacturers

A clear message from FDA's guidance is that manufacturers that have not already done so should incorporate cybersecurity considerations into their design control procedures. Manufacturers should also expect questions from FDA regarding their risk analysis of cybersecurity considerations during the agency's review of premarket submissions. Moreover, manufacturers should evaluate whether any security enhancements are warranted for their currently marketed devices.

One aspect of the cybersecurity risk analysis that FDA recommends device manufacturers undertake is an identification of "residual" risks that cannot be directly mitigated by device design features. This aspect of the guidance recognizes that device security cannot be assured entirely by manufacturers, but is instead a "shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices."

The release of FDA's final guidance comes a week after FDA's announcement of a public workshop to be held on October 21-22, 2014, to discuss collaborative approaches for medical device and healthcare cybersecurity. The public workshop will seek broad input from the healthcare and public health sector on the development of processes and best practices to strengthen medical device cybersecurity. As the announcement of this workshop illustrates, implementing FDA's final guidance is likely to involve a learning process for both device manufacturers and the agency.

Ropes & Gray will continue to monitor developments in this area. If you have any questions, please contact any member of Ropes & Gray's FDA regulatory practice or your usual Ropes & Gray Advisor.

[1] Curiously, the Federal Register notice announcing the availability of FDA's final guidance still includes the "to maintain information confidentiality, integrity, and availability" language.