WILMERHALE

FDA Issues Draft Guidance on Cybersecurity Considerations in Premarket Submissions for Medical Devices

2013-06-20

On June 14, the Food and Drug Administration ("FDA") issued draft guidance on the content of premarket submissions for management of cybersecurity in medical devices.[1] Reflecting growing concerns both in the government and in the private sector about IT vulnerabilities in the increasing number of networked medical devices, the draft guidance identifies a series of cybersecurity considerations manufacturers should address during the design phase of devices and cybersecurity risk mitigation assessments they should document in their premarket submissions. Comments on the draft guidance—which applies to premarket notifications, premarket approval applications, product development protocols, and humanitarian device exemptions—are due September 12, 2013.

Background

FDA last directly addressed the issue of cybersecurity in the device approval process in 2005, when it issued guidance documents on cybersecurity for medical devices containing off-the-shelf software and on the content of premarket submissions for software contained in medical devices.[2] The first offered 10 basic questions and answers that highlighted the need to consider cybersecurity vulnerabilities in devices using off-the-shelf software under the framework of the Quality System Regulation (21 C.F.R. part 820), especially with respect to introduction of software patches. The second outlined the type and extent of documentation required in premarket submissions, depending particularly on the level of concern posed by a software malfunction.

Since those guidance documents were issued, the number of networked medical devices has exploded, as has the number of medical applications for mobile devices. In response, many federal bodies—including, for example, in the last 18 months, the Commerce Department's Information Security and Privacy Advisory Board, the Department of Homeland Security's ("DHS") National Cybersecurity and Communications Integration Center, and the Government Accountability Office ("GAO")—have raised concerns about what DHS has called the growing "attack surface" presented by medical devices to cyber attacks.[3] They have accordingly urged FDA to provide for more rigorous scrutiny of the cybersecurity risks presented by devices.

Guidance

The draft guidance represents FDA's response to those recommendations. The draft guidance's nonbinding instructions would encourage manufacturers

- to consider cybersecurity during the design phase of medical devices;
- to define and document the following components of their cybersecurity risk analysis and management plan as part of the risk analysis required under the Quality System Regulation:
    - identification of assets, threats and vulnerabilities,
    - impact assessment of threats and vulnerabilities on device functionality,
    - assessment of the likelihood of a threat or vulnerability being exploited,
    - determination of risk levels and suitable mitigation strategies, and
    - residual risk assessment and risk acceptance criteria;
- consider the balance between cybersecurity safeguards and the usability of the device in its intended use environment; and
- consider appropriate security control methods and provide justification in premarket submissions for controls chosen, such as various methods of
    - limiting access to trusted users,
    - ensuring trusted content, and
    - building in fail safe and recovery features.

Finally, the draft guidance provides a list of specific information that should be included in premarket submissions:

- hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with the device, including:
    - a list of all cybersecurity risks considered in the design of the device,
    - a list of and justification for cybersecurity controls employed;
- a "traceability matrix" linking cybersecurity risks and cybersecurity controls;
- a plan for providing updates and patches for operational systems and software;
- documentation demonstrating that the device will be provided to purchasers and users free of malware; and
- product specifications and instructions for use of anti-virus software and/or firewalls appropriate for the use environment.

Context

The draft guidance stands at the intersection of two increasingly important regulatory trends that reflect basic technological and economic shifts: the proliferation of cybersecurity standards and the development of guidelines for the movement of nearly every aspect of medical practice into the digital domain. As with the draft guidance on mobile medical applications issued by FDA in July 2011, but still not finalized,[4] the draft guidance on cybersecurity for medical devices provides an opportunity for manufacturers, purchasers, practitioners, and patients to contribute to the shaping of this important regulatory development.

---

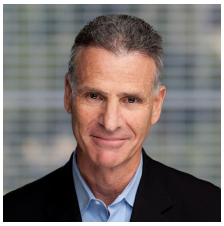
[1] The draft guidance is available here: http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356186.htm, or here: http://www.regulations.gov/#!documentDetail;D=FDA-2013-D-0616-0001.

[2] Those earlier guidance documents are available here: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm; http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm.

[3] Department of Homeland Security, National Cybersecurity and Communications Integration Center, Attack Surface: Healthcare and Public Health Sector (May 2012), available at http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf; see Information Security and Privacy Advisory Board, Letter to the Honorable Jeffrey Zients, Acting Director, Office of Management and Budget (Mar. 30, 2012), available at http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-ltr-to-omb_med_device.pdf; Government Accountability Office, FDA Should Expand Its Consideration of Information Security for Certain Types of Devices (Aug. 2012), available at http://www.gao.gov/products/GAO-12-816.

[4] That draft guidance is available here: http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm263280.htm.

Authors



Bruce S. Manheim Jr.

PARTNER

bruce.manheim@wilmerhale.com

+1 212 230 8817