Morgan Lewis

alert

life sciences and healthcare lawflash
from the FDA Practice

June 17, 2013

FDA Taking on Cybersecurity Risks for Medical Devices

FDA issues safety communication and draft guidance clarifying that manufacturers are responsible for addressing cybersecurity risks related to their medical devices.

On June 13, in response to increased reports of computer viruses and other cybersecurity breaches concerning medical devices and hospital networks, the Food and Drug Administration (FDA) issued a safety communication on cybersecurity for medical devices and hospital networks[1] and a new draft guidance document, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."[2] As software has become increasingly prevalent in medical devices, allowing for more sophisticated uses and networked connectivity, the cybersecurity risks for these devices also have increased. Recognizing that these risks may impact device performance and safety, FDA clarified that device manufacturers are responsible for identifying and mitigating cybersecurity risks for their medical device products. Although the new draft guidance makes clear that FDA expects device manufacturers to evaluate and address these issues for new devices going forward, questions remain as to the extent of manufacturers' obligations for cybersecurity risks affecting older devices, particularly with respect to discontinued devices that are still in use but are no longer supported by a device manufacturer.

Medical Device Cybersecurity: The Focus of Broader Efforts Across Agencies

FDA's actions appear to be part of a more comprehensive response to medical device cybersecurity concerns identified by the Obama administration. For example, in May 2012, the Department of Homeland Security (DHS) issued a bulletin stating that, because wireless medical devices are now connected to hospital and other healthcare facility information technology (IT) networks, "IT networks are now remotely accessible through the [medical device]," creating new vulnerabilities for these networks.[3] The U.S. Government Accountability Office (GAO) also identified information security threats for certain medical devices in a report issued in August 2012, which recommended that FDA develop and implement a plan expanding its focus on these types of information security risks.[4]

Subsequently, in February 2013, the Obama administration initiated a coordinated effort to address cybersecurity concerns through the issuance of an executive order and a presidential policy directive. Executive Order 13636 directs the National Institute of Standards and Technology to develop a framework to reduce cyber risks to critical infrastructure.[5] The presidential policy directive "Critical Infrastructure Security and Resilience" granted DHS the authority to identify cyber threats, vulnerabilities, and consequences.[6] DHS has created an Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to implement the presidential policy directive by working to "reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors." One of ICS-CERT's 16 identified critical infrastructure sectors is

1. View the safety communication at http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm.
2. View the draft guidance at http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm.
3. View DHS's bulletin at http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf.
4. View GAO's report at http://gao.gov/assets/650/647767.pdf.
5. View the executive order at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
6. View the presidential policy directive at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

the “Healthcare and Public Health Sector,” for which the Department of Health and Human Services is designated as the sector-specific agency. Additionally, DHS has identified “medical device and supply companies” as one of the major elements of the Healthcare and Public Health Sector.

Recommendations in FDA’s New Draft Guidance

FDA’s new draft guidance is intended to provide recommendations on the type of documentation that device manufacturers preparing premarket submissions should include to address cybersecurity risks that may compromise device functionality. The draft guidance applies to premarket 510(k) submissions, de novo petitions, premarket approval applications, product development protocols, and humanitarian device exemptions. Additionally, FDA encourages manufacturers to apply the draft guidance principles to investigational device exemption submissions and devices exempt from premarket review.

Although FDA acknowledges that the extent of security controls will depend on the medical device, its use environment, and the risks presented to patients by a potential security breach, the draft guidance includes several general recommendations. Manufacturers are encouraged to justify, in their submissions, the security controls chosen, including the following: (1) limiting access to trusted users only, particularly for life-sustaining devices or devices that could be directly connected to hospital networks; (2) ensuring the trusted content of software by restricting software and firmware updates to authenticated code, using systematic procedures for authorized users to download the manufacturer’s software and firmware, and ensuring secure data transfer to and from the device; (3) using “fail safe” modes to maintain a device’s critical functionality, even when the device’s security has been compromised.

FDA also recommends that manufacturers include the following with their submissions: (1) a hazard analysis, mitigations, and design considerations to identify and control cybersecurity risks; (2) a traceability matrix linking actual cybersecurity controls to the risks considered; (3) a systematic plan for providing validated updates and patches to operating systems or software to update the protections; (4) documentation to demonstrate that the device will be provided free of malware to purchasers and users; and (5) instructions for use and specifications related to antivirus software and/or firewall use appropriate for the device and its use environment.

Considerations for Evaluating Device Manufacturers’ Cybersecurity Responsibilities

In evaluating the impact of these new cybersecurity initiatives, device manufacturers should be mindful that FDA is not the only agency pursuing these issues. While FDA has direct authority over the regulation of medical devices, there have been reports that DHS may be coordinating with FDA and interacting with device manufacturers to encourage implementation of controls against cybersecurity threats. FDA also mentioned DHS in its safety communication and provided a link to the DHS ICS-CERT website. Thus, although DHS may not have direct regulatory authority to require the implementation of changes or new controls to address device cybersecurity, if device manufacturers are contacted directly by DHS, they should consider DHS’s coordination with FDA and FDA’s express statements concerning the impact of cybersecurity risks on device safety.

Manufacturers also should consider the impact of FDA’s and DHS’s focus on device cybersecurity on older, existing devices. While the draft guidance provides recommendations for the development and premarket review of new devices, FDA has not provided express guidance on its expectations for existing devices. For example, it is still uncertain to what extent FDA would expect device manufacturers to modify existing devices to address cybersecurity risks, particularly for older devices that may be near the end of their useful life. Further, although FDA stated in its safety communication that “FDA typically does not need to review or approve medical device software changes made solely to strengthen cybersecurity,” it is not clear the extent to which FDA would agree that such changes do not have the potential to affect the device’s performance or safety.

Comments on the FDA draft guidance should be submitted by September 12, 2013 to be considered before work begins on the final guidance.

Contacts

If you have any questions on the issues discussed in this LawFlash or would like assistance in preparing comments to FDA, please contact the authors of this LawFlash, **M. Elizabeth Bierman** (202.739.5206; mebierman@morganlewis.com), **W. Reece Hirsch** (415.442.1422; rhirsch@morganlewis.com); or **Michele L. Buenafe** (202.739.6326; mbuenafe@morganlewis.com).

About Morgan, Lewis & Bockius LLP

With 24 offices across the United States, Europe, and Asia, Morgan Lewis provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. Our international team of lawyers, patent agents, benefits advisers, regulatory scientists, and other specialists—more than 1,600 legal professionals total—serves clients from locations in Almaty, Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Moscow, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.