FDA Alerts Medical Device Manufacturers and Hospitals to Cybersecurity Risks

On June 13, 2013, the Food and Drug Administration ("FDA") issued an alert and draft guidance recommending that medical device manufacturers and health care facilities take measures to protect against cyberattacks that could compromise device performance and patient safety. The alert identifies specific cybersecurity risks associated with medical devices, including the introduction of malware into medical equipment or unauthorized access to devices' configuration settings. The draft guidance focuses on the development and documentation of cybersecurity management in medical device premarket submissions.

Medical Device Cybersecurity Incidents and Vulnerabilities

FDA's alert is directed to medical device manufacturers, hospitals and other device user facilities, health care IT and procurement staff, and biomedical engineers. It explains that medical devices can be vulnerable to cybersecurity breaches because they often contain configurable embedded computer software and are increasingly interconnected through the Internet, smart phones and hospital networks.

Although FDA is not currently aware of any deaths or patient injuries associated with cybersecurity breaches, or that any device or system has been "purposely targeted," it has become aware of cybersecurity "incidents" and "vulnerabilities." These include the presence of malware, failure to provide security software updates, and uncontrolled distribution of passwords for privileged device access.

According to *The Wall Street Journal*, Department of Veterans Affairs records indicate that malware has affected at least 327 medical devices at VA hospitals since 2009, and that during a single outbreak in February 2012, the notorious Conficker malware was detected on 104 devices at a VA Hospital in Tampa, Florida.[1] Such computer infections can consume a device's processing power or potentially expose patients' names and past medical procedures. In addition, in conjunction with FDA's alert, the Department of Homeland Security issued a separate alert warning that an estimated 300 medical devices from 40 vendors could be vulnerable to hacking and that "the vulnerability could be exploited to potentially change critical settings and/or modify device firmware."[2]

Mitigating Risk of a Cybersecurity Breach

The FDA alert explains that medical device manufacturers are responsible for identifying cybersecurity risks associated with their devices and recommends specific measures that medical device manufacturers, as well as health care facilities, should take to identify and address potential cybersecurity vulnerabilities. The alert's recommendations to medical device manufacturers developing new devices align with those set forth in the draft guidance. However, the alert signals regulatory flexibility with respect to changes made to existing devices, stating that "FDA typically does not need to review or approve medical device software changes made solely to strengthen cybersecurity."

Draft Guidance on Cybersecurity Development in Premarket Submissions

FDA's draft guidance provides recommendations for device manufacturers to "consider and document" in premarket submissions, including (i) premarket notifications (510(k)s); (ii) *de novo* petitions; (iii) premarket approval applications (PMAs); (iv) product development protocols (PDPs); and (v) humanitarian device

[1] *See* "Patients Put at Risk By Computer Viruses", WSJ.com (last visited June 13, 2013) *available* here.
[2] *See* Alert (ICS-ALERT-13-164-01), Medical Devices Hard-Coded Passwords (June 13, 2013) *available* here.

exemption (HDE) applications. It defines cybersecurity as the "process of preventing unauthorized modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient." The guidance recommends that cybersecurity controls should be developed during the design phase and suggests that manufacturers define and document cybersecurity measures as part of their risk analysis pursuant to 21 C.F.R. § 820.30(g).

The draft guidance recognizes that the extent of security controls depends on factors such as the design of the device, its environment for use, the risk of security breach, and risk to patients from a security breach. It also notes that medical devices connected to the Internet or to other devices are at a higher risk of a cybersecurity breach.

Based upon such factors, FDA recommends that manufacturers justify in their premarket submissions the security controls chosen for a device. Appropriate security controls may include (i) limiting access to trusted users only; (ii) 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; and (iii) use of "fail safe" and recovery features that protect the device's critical functionality, even when the device's security has been compromised.

Finally, the draft guidance outlines specific cybersecurity information that medical device manufactures should include in premarket submissions. The information includes identifying specific cybersecurity risks and the corresponding controls designed to mitigate such risks, including submission of a hazard analysis and traceability matrix linking specific cybersecurity risks to specific controls. Additionally, the agency recommends submitting documentation to show that the device will be free of malware when purchased by users, as well as instructions for use and specifications related to recommended antivirus software.

Consequences for Medical Device Manufacturers

FDA's alert and draft guidance have implications that go beyond the premarket submissions. While the draft guidance applies only to premarket submissions, the alert indicates that medical device manufacturers have responsibility for ensuring security of existing devices. Medical device manufacturers may want to consider conducting a retrospective audit of the cybersecurity measures on their existing devices in addition to updating their design control procedures to ensure that cybersecurity is appropriately considered when developing future devices.

Another cybersecurity consideration is the recent application of the HIPAA Security Rule to companies that provide device-related services to HIPAA covered entities such as hospitals and physician offices. In the HIPAA Omnibus Rule issued in January 2013, the Department of Health and Human Services clarified that medical device manufacturers, and companies that service medical devices, will be considered business associates of covered entities when they service devices that provide access to protected health information. As business associates, such entities will be subject to additional cybersecurity requirements. Business associates will have until September 23, 2013, to determine, and adopt, the steps needed for compliance.

Recommendations for Health Care Facilities

As part of its alert, FDA also reminds health care facilities to evaluate their own network security and protect their computer systems that are used in connection with medical devices. FDA's recommendations to health care facilities are consistent with the HIPAA Security Rule, already applicable to covered entities, and include (i) restricting unauthorized access to the network and networked medical devices; (ii) making certain

appropriate antivirus software and firewalls are up-to-date; (iii) monitoring network activity for unauthorized use; (iv) protecting individual network components through routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services; and (v) developing and evaluating strategies to maintain critical functionality during adverse conditions. In addition, health care providers are advised to contact the medical device manufacturer if they believe there might be a cybersecurity problem related to a device.

FDA will be accepting comments on the draft guidance until September 12, 2013. For more information, please contact a member of Ropes & Gray's FDA regulatory team or your regular Ropes & Gray attorney.