ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM JUNE 20, 2013

Cyber Attacks on Human Health? FDA Urges Manufacturers to Tighten Cybersecurity on Medical Devices

By Kim Peretti and Cathy Burgess

Contributors: Lou Dennig and Brendan Carroll

The U.S. Food and Drug Administration (FDA) is the latest government agency to respond to the growing concern over increasing cybersecurity threats. After security analysts alerted FDA that medical devices used in the clinical setting were vulnerable to function manipulation and/or failure due to malware and other types of cyber threats, on June 13, 2013, FDA issued an FDA Safety Communication[1] in order to assist medical device manufacturers and health care facilities in ensuring that appropriate safeguards are in place to reduce the risk of device failure or compromise due to a cyberattack. The following day, FDA released draft guidance entitled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" ("Draft Guidance"),[2] which describes FDA's current thinking regarding cybersecurity features that should be developed in order to ensure that the functionality of a device is not compromised.

Although FDA is aware of no specific devices or systems that have been purposely targeted, and no deaths or injuries associated with these incidents have occurred, FDA has concerns that the rise in cybercrime makes these threats more likely. With an increasing number of medical devices operating as wireless, Internet- and network-connected devices, and with universal electronic transmission of medical device-related health information, the risk of computer viruses and other malware and unauthorized access to such devices increases. Vulnerabilities in cybersecurity may represent a risk to the safe and effective operation of networked medical devices, and failure to properly address these vulnerabilities could adversely affect patient care. The theft or loss of patient information also represents a significant risk to patient safety.

The Draft Guidance provides recommendations on development of security controls to ensure the confidentiality, integrity and availability of medical device data. Specifically, the Draft Guidance states that manufacturers should develop cybersecurity capabilities during the medical device design phase, then define and document components of their cybersecurity risk analysis and management plan as part of the risk analysis requirement

---

1 *See* "FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks" (June 13, 2013), *available at* http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm.

2 *See* "Draft Guidance for Industry and Food and Drug Administration Staff: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (June 14, 2013), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.

for design controls under 21 C.F.R. §820.30(g). As part of the risk analysis, the Draft Guidance recommends that manufacturers provide justification for security controls that they choose to incorporate in the medical device, such as limiting access to trusted users, ensuring trusted content and using fail-safe and recovery features.

The Draft Guidance identifies cybersecurity documentation that should be included in a premarket submission, such as a hazard analysis of the intentional and unintentional risks associated with the device, a traceability matrix linking cybersecurity controls to cybersecurity risks, device instructions and specifications related to antivirus software, and the manufacturer's plan for providing validated upgrades and operating system or software patches.

FDA's proactive approach continues a recent trend of increased regulatory interest in gathering information on cybersecurity controls and risks prior to a data compromise event. While most states require notification to customers, the state attorneys general office, or both, in the event of a compromise to the individual's personal information, those statutes are reactive and apply only in the event of a data breach. Last month, New York Governor Andrew M. Cuomo took action that required major health insurance companies operating in New York to divulge information regarding their cybersecurity controls regardless of whether they had been subject to a data breach.[3] Earlier this year, New York took similar action with regard to large banks operating in the state. FDA is the latest regulator seeking cybersecurity information before an incident occurs to ensure adequate protections are firmly in place.

It appears that FDA's cybersecurity recommendations have the potential to raise the bar for premarket submissions and add another layer of complexity to device development. Moreover, for premarket notifications, the guidance raises questions for substantial equivalence determinations. In other words, if the device is substantially equivalent to a predicate device, but fails to provide the cybersecurity controls described in the guidance, will FDA clear the device? The draft guidance also seems to raise the bar for products liability litigation in the event manufacturers fail to develop the types of controls described in the draft guidance.

Another complication is whether hospitals or manufacturers will be responsible for providing IT support. In its Safety Communication, FDA encourages health care facilities to evaluate network security in order to protect hospital networks from cybersecurity attacks. Such measures include monitoring network activity for unauthorized access or use, updating antivirus software and firewalls, updating security patches and disabling all unnecessary ports and services for each individual network component and developing strategies to maintain critical functionality under adverse conditions.

FDA's Draft Guidance signals the agency's intention to minimize the threat of cybersecurity risks through more stringent regulatory oversight in the medical device arena. Industry has the opportunity assist the agency in crafting recommendations that not only protect patient safety, but also make good business sense. Comments on the Draft Guidance are due by September 12, 2013.

Security Incident Management & Response Team Co-Chairs

Kim Peretti | 202.239.3720 | kimberly.peretti@alston.com

Jim Harvey | 404.881.7328 | jim.harvey@alston.com

---

[3] *See* "New York State Inquires into Insurance Company Cybersecurity Practices: A Signal of Increased Proactive Regulator Interest in Data Security?" (June 4, 2013), *available at* http://www.alston.com/files/publication/b9785fea-f457-46b8-9739-e1c558ff2d63/presentation/publicationattachment/61c0d644-bb3f-49f9-a1f4-ecea6a9defce/cyber-alert-new-york-state-inquiries-into-insurance-company-cybersecurity-practices.pdf.