Cyber security Update

(my collection of thoughts)

John F Murray Jr
US Food & Drug Administration

November 29th, 2012

The FDA has communicated this information to industry and hospital facilities

- FDA issued guidance in 2005 [Guidance to Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software]—which answers question about pre-market review as well as other manufacturer responsibilities, such as validating software changes before releasing them.
- At the same time as the guidance, the FDA issued Information for Health care Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software" that describes FDA's concerns about cybersecurity and what the guidance document covers

- In April 2005, the FDA hosted a webinar on the cybersecurity. The transcript is available at http://www.fda.gov/MedicalDevices/Safety/MedSunMedicalProductSafetyNetwork/ucm127816.htm
- In November 2009, the FDA issued Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility that reminded device manufacturers, hospitals, medical device users facilities, healthcare IT and procurement staff, medical device users, and biomedical engineers of the 2005 guidance as well as simple ways to protect against cybersecurity threats.
-

After publishing a guidance

- on cybersecurity in 2005, the FDA recognized that cybersecurity is a shared risk environment that involved more than just medical device manufacturers. The 80001 standard was designed address the cybersecurity issues related to the integration of medical devices and information technology (IT) systems, focusing on the shared risk of the manufacturers and the users of the device. We contributed to the 80001 global standard recently published and have helped design the security annex to it as well as technical reports on the application of the standard. We spoke about 80001 at the AAMI international standards meeting last year and again this year, and will continue to look at ways to improve software security/quality.

Has the FDA received any MDRs related to software hacking or cybersecurity?

- We have received one MDR report indicating a potential cybersecurity risk to medical devices. However, we have not received any reports that indicate that medical devices have actually been hacked while in use by a patient. While we receive MDRs related to software issues, the reports indicate software error/malfunction issues and not cybersecurity/hacking breaches.

FDA Key Messages

- The FDA is concerned about the security and privacy of medical devices, and has been emphasizing to manufacturers the importance of security as a key element in device design since our 2005 guidance on cybersecurity.
- Patients should realize that the benefits of using their medical device outweigh the current risks posed by cybersecurity threats, including hacking. FDA's current adverse event data do not indicate that breaches of device security measures represent a widespread problem

GAO Report

- In August 2012, the GAO released a report on cybersecurity: *Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices (GAO-12-816).*

- The GAO report recommends that the FDA develop and implement a more comprehensive plan to assist the agency in enhancing its review and surveillance of medical devices, as technology evolves, and that will incorporate the multiple aspects of information security.

GAO recommendation

- Increase its focus on manufacturers' identification of potential unintentional and intentional threats, vulnerabilities, and resulting information security risk, and strategies to mitigate these risks during its PMA review process;
- Utilize available resources, including those from other entities, such as other federal agencies;
- Leverage its postmarket efforts to identify and investigate information security problems; and
- Establish a specific schedule for completing this review and implementing these changes

Activity underway

- Conducting a systematic evaluation of how we review the software that supports new medical devices;
- Expanding FDA's national electronic safety tracking system to include medical devices;
- Developing global standards related to the integration of medical devices and information technology systems, focusing on the shared risk of both the manufacturers and the users of the device; and
- Strengthening our ability to detect medical device performance and safety issues as they occur

What is the FDA doing

- **to enhance the expertise of reviewers and scientists on these topics and collaborate with stakeholders?**
- The FDA works closely with academia with the goal of staying ahead of the technological curve.
- As part of our regulatory science program, we are developing techniques and laboratory expertise to assist us in identifying potential vulnerabilities and evaluating risk mitigation measures employed by regulated industry. Specifically, we are looking at ways to better detect malware inside device designs, and reverse engineering certain types of malware to best identify the specific protective practices that manufacturers could employ

How is the FDA specifically

- **working and collaborating with federal partners?**
- The FDA is engaged in setting consensus standards for the cybersecurity of medical devices and we actively work with federal colleagues who have authority over privacy evaluations. We continue to identify and leverage available resources in an effort to keep pace with technological innovation. Current efforts include establishing collaborative relationships with the Department of Homeland Security, the National Institute of Standards and Technology, the Department of Defense, and federal law enforcement agencies

The FDA is also planning

- a series of public meetings in partnership with the Office of the National Coordinator for Health Information Technology (ONC) and the Federal Communications Commission (FCC) to discuss current regulatory roles, identify areas of regulatory overlap and dialogue with external stakeholders and experts about the FDA's role in health information technology (HIT) related to medical devices. These meetings will help inform a report detailing the FDA's proposed strategy and recommendations on the regulatory framework for medical device HIT that both protects and promotes the public health and supports innovation. This report addresses Section 618 in FDASIA and also addresses the GAO recommendation that the FDA develop regulatory strategies for medical device cybersecurity

How can manufacturers

- **collaborate in this process?**
- Manufacturers are responsible for identifying risks and hazards associated with medical device software/firmware, including risks related to security, and are responsible for putting appropriate mitigations in place to address patient safety. While information related to theoretical device security problems is helpful, it is very important that the agency also receive reports of devices that have had security breaches. We are committed to working with industry to identify potential vulnerabilities and evaluate risk mitigation measures

How is FDA working on standard setting?

- The FDA continues to examine its consensus standards strategy in the area of wearable and implanted devices, including using and adapting available standards from other vulnerable sectors, such as industrial control (a set of devices managing, commanding, directing or regulating the behavior of other device(s) or system(s). CDRH has engaged with stakeholders to begin the process of studying what is available from other sectors and, where appropriate, tailoring it to the health sector.

How is FDA enhancing postmarket surveillance efforts?

- Device post-market efforts involve evaluating and enhancing surveillance tools that find and investigate information security problems. The following two initiatives will enhance postmarket surveillance efforts that will monitor targeted risk areas such as current and future information security oversight needs.
- CDRH's "Strengthening Our National System for Medical Device Postmarket Surveillance"

In September the FDA released

- Strengthening Our National System for Medical Device Postmarket Surveillance designed in part to strengthen national coordination of information sharing for adverse events related to medical devices. Included is this plan are specific actions to modernize adverse event reporting and analysis, which can help in the timely detection of adverse events that may be related to cybersecurity. The FDA proposes to increase reporting through automated adverse event reporting for facilities, increased electronic reporting, and a mobile medical apps for voluntary reporting from health care providers and consumers. To enhance our ability to detect safety signals, the FDA is developing a more robust database with modern analytic and search capabilities.

Expansion of FDA's Sentinel initiative

- to include devices
- The recently passed Food and Drug Administration Safety and Innovation Act (FDASIA) added medical devices the Sentinel Intiative, which draws on existing automated healthcare data from multiple sources to actively monitor the safety of medical products continuously and in real-time. Sentinel will provide FDA with the ability to analyze information collected during the course of routine health care, such as data from electronic health record systems, administrative and insurance claims databases and medical registries.

- The FDA is currently conducting a systematic review of our current practices in the pre-market review of medical device software, including the security of networked devices. The review will be completed and draft report issued by the end of the year. The information from this review will help inform our cybersecurity policy.