Pepper Hamilton LLP
Attorneys at Law

Client Alert
June 24, 2013

Berwyn | Boston | Detroit | Harrisburg | Los Angeles | New York | Orange County | Philadelphia | Pittsburgh | Princeton | Washington, D.C. | Wilmington

Unhack My Heart: FDA Issues Guidance to Mitigate Cybersecurity Threats in Medical Devices

Sharon R. Klein | kleins@pepperlaw.com
Odia Kagan | kagano@pepperlaw.com

A new guidance document from the FDA lists considerations and suggested steps to reduce the likelihood of cybersecurity breaches in medical devices.

In an especially edge-of-the-seat episode of the television drama "Homeland," a terrorist succeeds in remotely hacking into the pacemaker of the Vice President of the United States using the device's serial number. The terrorist then proceeds to induce a fatal heart attack by manipulating the device. Despite sounding much like science fiction, due to present-day technology and the connectivity of medical devices, this piece of fiction is indeed not too far from reality.[1]

On June 14, 2013, the Food and Drug Administration (FDA) issued for comment within 90 days, a draft guidance (Guidance) on the Management of Cybersecurity in Medical Devices.[2] The Guidance supplements the FDA's "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices" published on May 11, 2005[3] and the FDA's "Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (COTS) Software" published on January 14, 2005.[4]

In the new Guidance, the FDA outlines its current thinking with respect to issues manufacturers of medical devices are to consider in designing medical devices in order to effectively reduce the chance of a cybersecurity breach to the device. The FDA has been vocal in advocating quality initiatives for medical devices containing software or programmable logic that can be vulnerable to cybersecurity incidents.[5] Cybersecurity risks are defined in the Guidance as the intentional or unintentional compromise of a device or the data stored in it through 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 FDA is advising health care facilities to evaluate their computer networks to eliminate malware and computer viruses that can contaminate medical devices.

Beyond the design phase, the recommendations in the Guidance specifically address several "premarket submissions" of medical device manufacturers to the FDA, namely: Premarket Notification (510(k)), *De novo* petitions, Premarket Approval Applications (PMA), Product Development Protocols (PDP) and Humanitarian Device Exemption (HDE) submissions.

The CIA of Information

As a general principle, medical device manufacturers should implement measures in the devices to ensure the *confidentiality*, *integrity*, and *availability* of information stored in them:

- *Confidentiality.* This means that data, information, or system structures should be accessible only to authorized persons and entities at authorized times and in an authorized manner.
- *Integrity.* This means that data and information should be accurate and complete and should not be improperly modified.
- *Availability.* This means that data, information, and information systems would be accessible and usable when needed: on a timely basis in the expected manner.

It would be most efficient, both for the FDA approval process and for the efficiency and effectiveness of managing a device's security, that the cybersecurity issues and risks be addressed and analyzed in the design phase. Among other things, manufacturers are encouraged to document the following, as part of the risk analysis required by FDA rules on design control for medical devices:[6]

- What are the assets, threats, and vulnerabilities to the device and what is their expected impact?
- How likely is it that a vulnerability would be exploited?
- Is such risk an acceptable one and what are possible mitigation strategies?
- What are potential residual risk and risk acceptance criteria?

Security Guidelines

The Guidance breaks down the general principles with certain recommended appropriate security controls for the medical devices, especially those that are life-sustaining or connected to hospital networks:

Limiting Access to Trusted Users

Authenticate. The device should be accessible only following appropriate user authentication (username, password, smart card, etc.).

- *Compartmentalize.* Different parts of the device may be accessible only to certain individuals, depending on their role.
- *Time-Out.* The device would have automated log-off (time-out) after a certain time or inactivity.
- *Passwords.* Authorized passwords would have sufficient length and complexity.
- *Update Controls.* Special controls may be necessary to permit software or firmware updates.
- *Physical Locks.* Physical locks may be necessary.

Trusted Content

- *Secure Data Transfer.* Data transfer to and from the device should be secured, including accepted methods for encryption, where appropriate.
- *Update Controls.* Updates should only be made using authenticated code, including code signature verification.

Fail-Safe and Recovery Measures

- *Identify.* It should be possible to recognize, log and act upon security compromises as they happen.
- *Fail-Safe Measures.* Even when the device's security has been compromised fail-safe device features should be in place to protect the device's critical functionality.

Access in Emergency

The FDA is wary of medical device security measures doing more harm than good in emergency situations. Therefore, the Guidance specifies that the extent to which security measures would be needed depends on the attributes of the specific device. More extensive measures would be needed for devices capable of connecting to other medical devices, to the Internet or another network, or to portable media (e.g., USB or CD). Security measures should be tailored to the target audience using the device so as not to hinder access to the device during an emergency situation.

When the Joplin tornado hit St. John's hospital in Kansas City in May 2011, causing the electricity to go out, doctors and nurses lost access to many of the vital medicines in the ER and in virtually every other department. The power outage had caused the metal cabinets where the drugs are kept to automatically lock.[7] Medical staff would be left in a similar predicament as a result of a hacker compromising software controlling cabinets normally accessed by user names and passwords. Such a hacker could also access the system in order to access contraband and controlled substances.

Documentation

The Guidance concludes by suggesting manufacturers should provide certain documentation as part of the premarket submission to the FDA. These documents include:

- *Risk Analysis.* Hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with the device, including: a list of the risks and a list and justification of the controls implemented to address such risks and how they are linked to the risks. (This should be in the form of a traceability matrix).

- *Update Control*. A description of the systematic plan for providing validated updates and patches to operating systems or medical device software, as needed, to provide up-to-date protection and to address the product life cycle.
- *Disabling Code*.
  - Appropriate documentation to demonstrate that the device will be provided to purchasers and users free of malware, and
  - Instructions for use and product specifications related to recommended anti-virus software and/or firewall use appropriate for the environment of use.

Pepper Point*: Manufacturers of medical devices, particularly those with the ability to connect to other devices or to the Internet, are well advised to take into account the FDA's new Guidance as early as possible in the design of their medical devices. Additionally, hospital systems connected to devices should be audited to eliminate malware (which can be transferred to a medical device) and to ensure restricted access to devices. Though the Guidance is presently only a non-binding recommendation, it implements existing legal requirements in connection with data security as well as the FDA premarket authorization process. In addition, beyond the legal prism, devices that are more secure from potential cybersecurity breaches may be better positioned to win the trust, reliance, and purchasing dollars of the relevant institutions and consumers.*

Endnotes

1. *See e.g.*: Barnaby Jack "Broken Hearts": How Plausible Was the Homeland Pacemaker Hack?" at http://blog.ioactive.com/2013/02/broken-hearts-how-plausible-was.html; and Barnaby J. Feder "A Heart Device Is Found Vulnerable to Hacker Attacks" March 12, 2008 at http://www.nytimes.com/2008/03/12/business/12heart-web.html?_r=0.
2. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.
3. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089593.pdf.
4. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf.
5. "U.S FDA Urges Protection of Medical Devices from Cyber Threats" June 13, 2013 at http://www.reuters.com/article/2013/06/13/devices-cybersecurity-fda-idUSL2N0EP1LR20130613.
6. 21 CFR 820.30(g).
7. http://www.kansascity.com/2011/06/18/2959600/condition-gray-inside-the-hospital.html#storylink=cpy.