FDA Offers Guidance on Cybersecurity and Medical Devices

Save to myBoK

By Liisa Thomas and Idara Udofia

The Food and Drug Administration (FDA) has joined other regulators in sounding a call for data protection and security in our rapidly digitizing world.

Studies reveal that many health providers' devices or systems have been breached without their knowledge of such breach or the associated vulnerabilities.[1] According to SANS Institute, medical devices are the primary cause for transferring malicious attacks to other networks or devices in the medical sector.[2] Moreover, the Department of Health and Human Services' recent investigation revealed over two dozen devices were vulnerable to exploitation by hackers.[3]

In response to these concerns, the FDA issued guidelines on cybersecurity for medical devices on October 2, 2014. The document, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (guidelines), encourages manufacturers to consider cybersecurity measures in developing medical devices.[4] The guidelines are based on the National Institute of Technology's (NIST) Core Framework.[5] Although not legally binding, the FDA has indicated that it will consider compliance with the guidelines when engaging in its premarket review of a medical device.

The FDA has indicated that it will expect to see specific information about cybersecurity in a company's premarket device submissions, such as:

1. Hazard analysis, mitigations, and design considerations about the device
2. A matrix that shows how the controls trace to those risks
3. A summary plan about updates and patches
4. A summary of controls in place to maintain device integrity
5. User instructions about product security controls (like using a firewall or having anti-virus software)

Five Core Functions Developed

When putting together this documentation, what should manufacturers consider? The FDA has provided a list of "recognized consensus standards" which should be helpful to device manufacturers. That list will be updated at www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm. The FDA has also set out five core functions that need to be addressed by devices:

- Identify
- Protect
- Detect
- Respond
- Recover

Identify, Understand, and Protect Against Cybersecurity Risks

The first step in developing secure medical devices is to identify potential exposure and then protect against that exposure. For example, the FDA notes that devices capable of wirelessly connecting to the Internet "are more vulnerable to cybersecurity threats than devices that are not connected."[6] The FDA thus recommends in its guidelines that security be tailored to the risk connected to the intended end-user and corresponding environment:

> The extent to which security controls are needed will depend on the device's intended use, the presence and intent of its electronic data interfaces, its intended environment of use, the type of cybersecurity vulnerabilities present, the likelihood the vulnerability will be exploited (either intentionally or unintentionally), and the probable risk of patient harm due to a cybersecurity breach.[7]

Examples of security measures to consider include, among other things: limiting access through user authentication; having session timers; using layered authorization dependent on a user's role; providing physical locks; and ensuring trusted content by having, for example, updates that require an authentication code.

The goal is to design secure medical devices using security measures that can efficiently handle actual, high-priority future risk. The FDA further emphasizes this point by recommending that manufacturers submit a traceability matrix that connects the cybersecurity controls to the considered risks. Notwithstanding, the FDA acknowledges that the security controls should be appropriate for the intended end-user, illustrating that overly burdensome controls in an emergency situation should be avoided.[8]

Understanding the specific cybersecurity needs compliments the next recommendation: to provide compatible controls. In fact, the FDA goes a step further and recommends manufacturers justify chosen controls during the premarket submission process, further highlighting the agency's desire for customized security measures.[9] For instance, to limit access the agency recommended strengthening password protection by avoiding passwords that are "hardcoded" or commonly used. The agency also pointed to encryptions to secure data transfers to and from devices to maintain secure content.

Detect Vulnerabilities and Threats, Then Respond and Recover

In addition to proactively reducing the risk of cyber threats, the FDA guidelines also recommend equipping devices with cybersecurity measures that can detect, respond, and recover from vulnerabilities and threats while operating in its environment. In making its recommendation, the FDA recognizes the need to preserve functionality while managing threats or resolving security loops. It recommends implementing features that recognize, log, and address security breaches "during normal use" and features that protect "critical functionality," despite a breach in security.[10]

In keeping with the premise that all stakeholders share a responsibility in establishing effective cybersecurity, the FDA further suggests using a feature that informs end-users of security compromises, where such notice would guide end-users to respond and resolve the cybersecurity issue.[11]

Although the listed approaches are recommendations, the FDA expressly states that if manufacturers decide to use other measures to achieve these goals, they should provide justification, indicating that the FDA has a vested interest in features that detect, respond, and recover from cybersecurity vulnerabilities and threats.

Ongoing Device Protection

The FDA has indicated that during the premarket review it will consider the extent to which cybersecurity controls manage and mitigate risk over the lifecycle of the device. For instance, the FDA guidelines suggest that manufacturers include a plan for providing software updates and patches throughout the lifecycle of the medical device to assure safety and effectiveness.

The FDA further advises manufacturers to submit a list of recommended security controls, such as anti-virus software or firewalls that are appropriate for the environments in which the devices will be used. Moreover, in the guidelines the FDA encourages manufacturers to provide a summary that describes how the cybersecurity in the device will be maintained over time.[12]

Read and Heed the Guidelines

Companies that develop products subject to FDA review will need to read and heed these new guidelines. The intended consequence is safer devices. There may be unintended consequences as well, beyond increased security compliance costs. For example, disclosing cybersecurity risks may impact manufacturer liability. The guidelines may also lead to the centralization within the FDA of information about cybersecurity risks and resolutions for medical devices.

Notes

[1] Finkle, Jim. “U.S. government probes medical devices for possible cyber flaws.” Reuters. October 22, 2014. www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022.

[2] Paganini, Pierluigi. “Risks and Cyber Threats to the Healthcare Industry.” Infosec Institute. September 16, 2014. http://resources.infosecinstitute.com/risks-cyber-threats-healthcare-industry/.

[3] Finkle, Jim. “U.S. government probes medical devices for possible cyber flaws.”

[4] US Food and Drug Administration. “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff.” October 2. 2014. www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.

[5] National Institute of Standards and Technology. “Draft – Framework Core.” www.nist.gov/itl/upload/draft_framework_core.pdf.

[6] US Food and Drug Administration. “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices...,” pg. 4.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Ibid, pg. 5.

[11] Ibid.

[12] Ibid, pg. 6.

Liisa Thomas (lmthomas@winston.com) is a partner at Winston and Strawn, and chair of the firm’s privacy and data security practice. She is an adjunct professor of privacy law, and the author of *Thomas on Data Breach: A Practical Guide to Handling Worldwide Data Breach Notifications*. Idara Udofia (iudofia@winston.com) is an associate in the Chicago office of Winston and Strawn.

Article citation:
Thomas, Liisa; Udofia, Idara. "FDA Offers Guidance on Cybersecurity and Medical Devices" *Journal of AHIMA* 86, no.2 (February 2015): 42-43.