PUBLICATION

FDA Recommends that Manufacturers Seeking Medical Device Approval Submit Cyber Security Plans [Ober|Kaler]

June 18, 2013

This article was reprinted in the June 28, 2013 issue of* Health Lawyers Weekly*, a publication of the American Health Law Association.

Last week, the FDA took steps to address a quietly growing concern regarding cyber security and medical devices. Specifically, the agency issued Draft Guidance requiring the submission of cyber security materials as part of any premarket submissions [PDF] and a Safety Communication explaining in more plain terms the scope of the cyber security issues addressed and the FDA's recommended actions. While the Draft Guidance may only apply to manufacturers who intend to submit premarket materials for approval, the Safety Communication is also targeted to, and should be reviewed by, hospitals that rely on medical devices and information networks threatened by malicious software (malware).

The Safety Communication

The latest Safety Communication echoes concerns that the FDA first enunciated in a November 2009 Communication. In essence, the new Communication expands on the previous Communication, and provides more specific guidance to users, purchasers, providers and manufacturers of medical devices. The guidance notes that the FDA has "recently" become aware of security risks to medical devices (and therefore to hospital operations). Specifically:

- Network connected or configured medical devices being affected by malware;
- The presence of malware on mobile electronics (including smartphones and tablets) used to access patient information, monitoring systems, and implanted devices;
- "Uncontrolled" distribution of passwords (including "hard-coded" passwords);
- Failure to provide timely security and similar software and firmware updates (and address security issues in older devices); and
- Security vulnerabilities in off-the-shelf software solutions designed to prevent unauthorized device or network access.

Although not specifically discussed in the Communication, the Communication was released on the same day as a *Wall Street Journal* article publicizing a series of infections at VA hospitals (*subscription may be required*), some of which were serious enough to impact hospital operations and even disable equipment. That article also noted at least one event in which the Office of Civil Rights was asked to investigate a GE radiology device at Beth Israel Deaconess Medical Center that had become infected and was apparently transferring patient information to a server outside of the hospital. (The server was never located.) It seems likely that the FDA's actions are meant to combat what appears to be a growing problem of cyber security and connected (or simply connectable) medical devices.

The Communication speaks to both manufacturers and health care facilities. For manufacturers (in addition to the Draft Guidance, discussed below) the Communication encourages the adoption of steps that will limit unauthorized device access (particularly for life-sustaining devices), protect medical devices and their components (including upgrading and patching existing security as necessary), provide designs that preserve core functions even during an attack and provide methods to recover and restore compromised devices. For facilities, the Communication recommends:

- Restricting unauthorized access to facility networks and networked devices;
- Ensuring that all security software is up to date;
- Monitoring network activity (for suspicious movement, such as a radiology device communicating with an outside server seemingly on its own initiative);
- Regularly reviewing security, updating as necessary, and disconnecting devices that do not require connections;
- Reaching out to manufacturers, the FDA, or DHS ICS-CERT where a vulnerability or problem is found; and
- Developing strategies to preserve critical functions during adverse conditions.

The Draft Guidance

The FDA's Draft Guidance applies to Premarket Notification (510(k)) including Traditional, Special, and Abbreviated 510(k) submissions; *De novo* petitions; Premarket Approval Applications (PMA); Product Development Protocols (PDP); and Humanitarian Device Exemption (HDE) submissions relating to medical devices that contain software, firmware, or programmable logic. In short, the guidance intends to ensure that medical devices will maintain information confidentiality, integrity and availability – even when infected with malware. To achieve these goals, the Draft Guidance recommends that manufacturers "consider cybersecurity during the design phase of the medical device, as this can result in more robust and efficient mitigation of cybersecurity risks." Specifically, manufacturers, as part of the risk analysis required in a pre-market submission, should define and document:

- An identification of assets, threats and vulnerabilities;
- An impact assessment of the threats and vulnerabilities on device functionality;
- An assessment of the likelihood of a threat and of a vulnerability being exploited;
- A determination of risk levels and suitable mitigation strategies; and
- A residual risk assessment and risk acceptance criteria.

The Draft Guidance goes on to address the security capabilities it expects to be described in premarket submissions and the documentation it recommends be used to evidence the existence of necessary security considerations.

Security Capabilities

The Draft Guidance acknowledges that the identification of appropriate security measures will be heavily dependent on context – how and where the device will be used, what features it offers, how it is accessed or maintained, etc. The Draft Guidance also notes an understanding that security features could compromise usability (especially, for instance, in an emergency) and that careful consideration of an appropriate balance is necessary. With these caveats in mind, however, the Draft Guidance recommends that premarket submissions include justification for the use (or exclusion) of certain security features, including (but not limited to):

- Requiring device access authentication (such as passwords, smart cards, or biometric identifiers);
- Automated timed log-offs;
- Providing support for layered authorizations (providing different users different levels of access);

- Requiring multi-factor authentication for privileged users (such as technicians who may alter software or firmware configurations);
- Avoiding "hard-coded" passwords (passwords that are the same for each device and difficult to change);
- Providing physical locks on both the device itself and its communication ports;
- Requiring user access authentication prior to permitting updates or other software modification;
- Restricting software modification to authenticated code, issued by the manufacturer and confirmed using that manufacturer's authentication system;
- Provide procedures for authorized users to download version-identifiable software and firmware from the manufacturer;
- Provide for secure data transfer to and from the device, using encryption technology as appropriate;
- Provide for "fail-safe" device features that protect the device's critical functionality, even when the device's security has been compromised;
- Provide features that allow for the recognition of an security breach (such as an infiltration of malware or other unwelcome code), logging, and corrective action;
- Provide methods of data and device recovery by an authenticated administrative user.

Documentation

In a premarket submission, the Draft Guidance recommends that manufacturers provide the following:

- An analysis of hazards posed, mitigations, and design consideration related to cyber security risks associated with the device (including "specific" listings of all risks that were considered during device design and all cyber security controls (and their justifications) established for the device);
- A "traceability matrix" linking security controls established with those that were considered;
- The systematic plan for providing validated software and firmware updates and patches;
- "Appropriate" documentation that the device will be provided to purchasers free of malware; and
- Device instructions and product specifications regarding recommended security environment steps (such as anti-virus software, firewall configuration and the like).

As always, the FDA's guidance is not legally binding – these steps are recommended, but not required. The guidance, however, provides clear insight into the agency's thoughts on appropriate manufacturer responses to cyber security threats and should not be ignored.

Ober|Kaler's Comments

That our increased dependence on networked, connected, and connectible devices requires increased vigilance comes as no surprise, but, many providers may be surprised to learn of the vulnerably of even "off-the-grid" devices. It is essential for enterprise security to remember that viruses and other malware (such as the now infamous STUXNET code) do not require an internet or intranet connection to spread – a single infected USB storage device, used to install updates, for instance, or to transfer or back-up patient data can easily become a digital Typhoid Mary, wreaking havoc throughout an organization without actually showing any signs of infection itself. The new FDA Draft Guidance raises the issue, but, especially for hospitals and other providers, an analysis of the risks presented by malware infection (and the potential for such infections to seriously compromise the confidentiality of protected health information), is already likely required under the HIPAA Privacy and Security Rules. Both manufacturers and end users, including providers, should review their policies and procedures to ensure that they properly account for the risks identified by the FDA.

* *Joshua J. Freemire is a former member of Ober|Kaler's Health Law Group*