Published on *The National Law Review* https://natlawreview.com

FDA Issues Final Guidance on Cybersecurity for Medical Devices

Article By:

Lynn C. Tyler, M.S.

FDA recently issued a final guidance document titled, “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.” FDA states that it developed the guidance to assist the industry by identifying issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices as well as in preparing premarket submissions for those devices. The implication is that, where applicable, medical devices will need to incorporate cybersecurity features to secure clearance or approval.

In the guidance, FDA notes that generally “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.”

The guidance further states that premarket submissions (including 510(k)s, PMAs, PDPs, HDEs, and de novo petitions) should justify the security controls chosen for their devices. The guidance provides the following exemplary list of controls to consider for identifying potential cyber threats and protecting against them:

Limit Access to Trusted Users Only

- Limit access to devices through the authentication of users (e.g., user ID and password, smartcard, biometric);
- Use automatic timed methods to terminate sessions where appropriate;
- Where appropriate, employ a layered authorization model by differentiating privileges based on the user role (e.g. caregiver, system administrator) or device role;
- Use appropriate authentication (e.g., multi-factor authentication to permit privileged device access to system administrators, service technicians, maintenance personnel);
- Strengthen password protection by avoiding “hardcoded” password or common words (i.e.

passwords which are the same for each device, difficult to change, and vulnerable to public disclosure) and limit public access to passwords used for privileged device access;

- Where appropriate, provide physical locks on devices and their communication ports to minimize tampering;

- Require user authentication or other appropriate controls before permitting software or firmware updates, including those affecting the operating system, applications and anti-malware.

Ensure Trusted Content

- Restrict software or firmware updates to authenticated code. One authentication method manufacturers may consider is code signature verification;

- Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer;

- Ensure capability of secure data transfer to and from the device, and when appropriate, use methods for encryption.

In the categories of detecting, recovering from and responding to cyber threats, the guidance suggests manufacturers consider the following:

- Implement features that allow for security compromises to be detected, recognized, logged, timed and acted upon during normal use;

- Develop and provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event;

- Implement device features that protect critical functionality, even when the device's cybersecurity has been compromised;

- Provide methods for retention and recovery of device configuration by an authenticated privileged user.

In premarket submissions, the guidance recommends that manufacturers address the following cybersecurity issues:

- Hazard analysis, mitigations and design considerations pertaining to intentional and unintentional cybersecurity risks associated with your device, including:

    - A specific list of all cybersecurity risks that were considered in the design of your device;

    - A specific list and justification for all cybersecurity controls that were established for your device.

- A traceability matrix that links your actual cybersecurity controls to the cybersecurity risks that were considered;
- A summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device to continue to assure its safety and effectiveness.
- A summary describing controls that are in place to assure that the medical device software will maintain its integrity (e.g., remain free of malware) from the point of origin to the point at which that device leaves the control of the manufacturer; and
- Device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g., anti-virus software, use of firewall).

A copy of the guidance can be found here.

National Law Review, Volume IV, Number 279