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

FDA Issues New Draft Cybersecurity Guidance for Medical Devices

Article By:

Shanna M. Pearce

The Food & Drug Administration has recently released for comment a draft expansion of guidance regarding Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Although the FDA issued existing guidance in 2014, the new guidance reflects concerns about the rapidly-changing nature of cybersecurity threats, and the potentially grave consequences of cybersecurity incidents involving healthcare and medical devices—particularly medical devices which connect to the internet, networks, or other devices. The draft guidance gives recommendations to medical device manufacturers about the device design, labeling, and documentation that the FDA expects to see in premarket submissions. It updates and expands beyond the prior guidance in several significant respects.

First, the draft guidance introduces a two-tiered classification of cybersecurity risk. Connected devices which, if compromised, could cause harm to multiple patients are considered the highest risk and are in "Tier 1." Examples of Tier 1 devices include pacemakers, dialysis devices, and insulin pumps, which are connected to systems such as home monitors or can be controlled externally. Premarket submissions for Tier 1 devices should include documentation about how the device design and risk assessment incorporate all of the FDA's recommended cybersecurity design controls. In Tier 2 are all other devices; manufacturers of Tier 2 devices may opt to include a risk-based rationale for why certain specific FDA-recommended cybersecurity design controls are not appropriate in lieu of documentation demonstrating that all controls have been incorporated.

Second, the draft guidance provides a framework, similar to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, for designing "trustworthy" devices. A trustworthy device is designed so as to prevent all unauthorized use, to ensure the integrity of the system's functionality and safety features, and to protect the confidentiality of data. Trustworthy devices should also be designed to timely identify cybersecurity events, to quickly respond to and contain the impact of a potential cybersecurity incident, and to recover capabilities or services impaired by an incident. The guidance provides a lengthy list of design controls intended to accomplish these goals, including the use of layered authorization, NIST standards of cryptography, a "deny by default" approach to connection, and the ability to update with software patches to address future vulnerabilities.

Third, the draft guidance recommends that manufacturers include a cybersecurity bill of materials

("CBOM") to be shared with customers. A CBOM is a list of commercial and/or off-the-shelf software and hardware components included in the device. The intent is to empower customers to take their own protective measures if any of those components are later discovered to have vulnerabilities.

Fourth, the draft guidance addresses the FDA's labeling regulations. FDA regulations require that device labeling includes directions for use, and the purposes and conditions of use, which include hazards, warnings, precautions, and contraindications. The draft guidance interprets the regulation's labeling requirement to include relevant security information. The FDA recommends fourteen items to be included in medical device labeling provided with premarket submissions, including a CBOM, instructions for downloading version-identifiable software and firmware from the manufacturer, instructions for how to respond upon detection of a cybersecurity vulnerability or incident, and, if known, information about when the manufacturer is expected to stop providing security patches or software updates.

Comments on the draft guidance are due by March 18, 2019. When finalized, the draft guidance will replace the 2014 guidance "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." However, it will not replace but only supplement the FDA's other related guidance documents—"Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices" (2005) and "Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software" (2005) will both remain in effect.

Putting it Into Practice: The new draft guidance demonstrates that the FDA expects medical device manufacturers, particularly of connected devices, to take a forward-thinking approach to cybersecurity early in the design process.

National Law Review, Volume VIII, Number 333