THOMSON REUTERS
Westlaw®

# Cybersecurity déjà vu

**By Adrienne R. Lenz, Esq., *Hyman, Phelps & McNamara****

**DECEMBER 11, 2018**

On October 18, FDA issued a new draft guidance document, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices ("Draft Guidance"). When final, it will supersede the 2014 guidance document of the same name ("Current Guidance").

The guidance comes shortly after release of the MITRE Corp.'s Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook, a document FDA contributed to, that is intended to guide healthcare delivery organizations in preparedness and response related to medical device cybersecurity incidents.

The topics we blogged about back then, including premature enforcement of a draft guidance and heightened requirements for establishing substantial equivalence of software devices reviewed in the 510(k) program, are concerns we have again with release of the Draft Guidance.

Back in 2013, we wrote that FDA appeared to be requesting cybersecurity information for software devices while the guidance was still a draft. We are again aware of recent additional information requests asking for more detailed cybersecurity information, beyond that described in the Current Guidance, and similar to that recommended in the Draft Guidance.

We also previously wrote that, for 510(k) devices, regardless of the predicate device's design or supporting documentation, FDA would expect to see substantial documentation related to the device's cybersecurity.

The Draft Guidance expands significantly the recommendations for cybersecurity design expectations, level of detail used in describing a device's cybersecurity considerations and the amount and type of documentation required in a premarket submission. It appears that 510(k) devices may again need to start meeting an even higher standard of cybersecurity to be considered substantially equivalent.

The Draft Guidance clarifies that it is applicable for "devices that contain software (including firmware) or programmable logic as well as software that is a medical device," Draft Guidance at 5.

It further defines two tiers of devices according to the cybersecurity risk, noting that the device's cybersecurity risk is different from the device's overall risk in determining its classification. Tier 1 is for devices with higher cybersecurity risk, defined as devices where the following criteria are met:

(1) The device is capable of connecting (e.g., wired, wirelessly) to another medical or non-medical product, or to a network, or to the Internet; AND

(2) A cybersecurity incident affecting the device could directly result in patient harm to multiple patients. *Id*. at 10.

A Tier 2 device is one that does not meet the Tier 1 criteria. For Tier 2 devices, the Draft Guidance recommends that sponsors include the documentation discussed for Tier 1 devices or "provide a risk-based rationale for why specific cybersecurity design controls" are not appropriate. *Id*. at 11.

The Draft Guidance expands significantly the recommendations for cybersecurity design expectations, level of detail used in describing a device's cybersecurity considerations and the amount and type of documentation required in a premarket submission.

The concept of an incident resulting in harm to "multiple patients" is new and not provided with any discussion. It will be interesting to see if FDA and sponsors reach different conclusions in terms of identifying types of cybersecurity incidents that could directly result in patient harm to multiple patients and thus whether a rationale will be acceptable or detailed design documentation will be needed in their premarket submission.

Like the Current Guidance, the Draft Guidance provides definitions, discussion of general principles related to cybersecurity controls and cybersecurity functions and cybersecurity documentation to be submitted in a premarket submission. However, the Draft Guidance expands in pages (from 7 to 24) and in detail related to device cybersecurity design, perhaps even being considered prescriptive.

Likewise, new information is recommended in device labeling related to cybersecurity and more detailed design and risk management documentation related to cybersecurity should be submitted in a premarket submission.

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

the answer company™
THOMSON REUTERS®

While there is a lot of new information in the Draft Guidance that could be discussed, two areas stand out: (i) the cybersecurity bill of materials (CBOM) and (ii) system diagrams.

The Draft Guidance defines a CBOM as "a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities" and recommends that the CBOM be included in the device labeling and submitted in premarket applications.

The Draft Guidance further recommends that the "device design should provide a CBOM in a machine readable, electronic format to be consumed automatically." *Id*. at 17. It is not clear whether some sponsors may consider this a disclosure of proprietary design information.

The Draft Guidance recommends that premarket submissions include:

> System Diagrams sufficiently detailed to permit an understanding of how the specific device design elements (from section V) are incorporated into a system-level and holistic picture. Analysis of the entire system is necessary to understand the manufacturer's threat model and the device within the larger ecosystem, *Id*. at 21.

For a large, complex software system, the amount of documentation will be extensive. Diagrams, however, may not necessarily be the best method of communicating the information. Unlike many recent guidance documents, the Draft Guidance does not include examples of diagrams to show what they should look like or how they might be used.

Such examples might have been helpful to sponsors evaluating how best to incorporate the recommendations into their design control procedures and design documentation.

As the recommendations in the Draft Guidance apply to the design of the device, sponsors will hopefully be provided a transition period to implement and validate recommended design expectations once the Draft Guidance is finalized. Unfortunately, no such transition is mentioned.

To the contrary, as noted above, we are already aware of requests for more detailed cybersecurity information in premarket submissions.

On that note, one recommendation in the Draft Guidance that sponsors may want to implement immediately is use of the pre-submission process to "discuss design considerations for meeting adequacy of cybersecurity risk management throughout the device life-cycle." *Id*. at 11.

* © 2018 Adrienne R. Lenz, Esq., Hyman, Phelps & McNamara

*This article first appeared in the December 11, 2018, edition of* Westlaw Journal Medical Devices.

## ABOUT THE AUTHOR

**Adrienne R. Lenz**, a senior medical device regulation expert at **Hyman, Phelps & McNamara** in Washington, provides consulting to medical device and combination product manufacturers. She assists clients with a wide range of pre- and post-market regulatory topics including developing regulatory strategy, preparing regulatory submissions, drafting regulatory policies and procedures, reviewing advertising and promotional materials, and addressing enforcement matters. She can be reached at alenz@hpm.com. This expert analysis was first published Oct. 30, 2018, on the firm's FDA Law Blog, www.fdablog.net. Republished with permission.

**Thomson Reuters** develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.