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

FDA Responds to Device Software Vulnerabilities by Releasing New Draft Cybersecurity Guidance

Article By:

Benjamin M. Zegarelli

On October 18, 2018, FDA released a new draft guidance, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, which describes the Agency's current thinking and recommendations on designing medical device software with adequate cybersecurity controls. Once finalized, the draft guidance will supersede a final guidance of the same name issued in 2014.

Although advances in device technology and software capabilities, along with increased incidence of cyberattacks in general, have elevated the priority of cybersecurity for FDA, the Agency's guidance is also a direct response to public reports that certain implantable devices (especially cardiac devices and infusion pumps) are susceptible to hacking. FDA has been working since the release of the final cybersecurity guidance in 2014 to track safety events involving software vulnerabilities and stay abreast of cybersecurity issues, as described on FDA's cybersecurity website. The new draft cybersecurity guidance aims to give manufacturers more detailed recommendations for integrating cybersecurity considerations into the device software design process.

More Substantial Cybersecurity Guidelines Tied to the QSR

In general, the updated guidance provides much more information on employing a risk-based cybersecurity analysis grounded in a functioning, compliant quality system. Through the guidance, FDA emphasizes the ties between cybersecurity design and the quality system regulation (QSR), 21 C.F.R. Part 820. This becomes apparent right away in the first substantive section, General Principles & Risk Assessment (renamed from General Principles in the 2014 guidance), in which FDA states "[a]s part of the software validation and risk analysis required by 21 C.F.R. 820.30(g), software device manufacturers may need to establish a cybersecurity vulnerability and management approach, where appropriate." While the 2014 guidance previously tied cybersecurity considerations to the QSR, the new draft guidance includes multiple references to a manufacturer's obligations under the QSR, making it clear that FDA does not see cybersecurity as an optional or simply recommended part of medical device software design. The new draft guidance also conveys FDA's expectation that consideration of cybersecurity risks is not a one-off design process but should continue throughout the product's lifecycle.

The new draft guidance introduces a new two-tiered approach to medical device cybersecurity requirements:

Tier 1 “Higher Cybersecurity Risk”

A device is a Tier 1 device if 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.

Examples of Tier 1 devices, include but are not limited to, implantable cardioverter defibrillators (ICDs), pacemakers, left ventricular assist devices (LVADs), brain stimulators and neurostimulators, dialysis devices, infusion and insulin pumps, and the supporting connected systems that interact with these devices, such as home monitors, and those with command and control functionality, such as programmers.

Tier 2 “Standard Cybersecurity Risk”

A medical device for which the criteria for a Tier 1 device are not met.

One question the new draft guidance does not answer explicitly, however, is whether standalone software devices (i.e., devices that are only software without a physical component, implantable or otherwise) can be Tier 1 devices. For instance, CADx devices intended to assist clinicians with diagnosing life-threatening illnesses and conditions could be vulnerable cyberattack that changes the software’s output such that it identifies additional or omits regions of interest, which could affect the diagnosis. Does this scenario mean CADx devices should be Tier 1?

FDA also recommends multiple new categories of cybersecurity considerations in the new draft guidance. Under the section, Identify and Protect Device Assets and Functionality, manufacturers should implement measures to: (1) “prevent unauthorized use,” (2) “ensure trusted content by maintaining code, data, and execution integrity,” and (3) “maintain confidentiality of data.” Under the section, Detect, Respond, Recover: Design Expectations, manufacturers should design the device software to: (1) “detect cybersecurity events in a timely fashion,” (2) “respond and contain the impact of a potential cybersecurity incident,” and (3) “recover capabilities or services that were impaired due to a cybersecurity incident.” The new draft guidance also includes recommendations for labeling devices with cybersecurity risks and for design and risk management documentation that should be included with pre-market submissions for Tier 1 and Tier 2 devices.

Cybersecurity is Growing as a Regulatory Requirement

While the 2014 final cybersecurity guidance is still in effect and will remain relevant until the new draft guidance is finalized, the new guidance paints a detailed picture about the direction FDA is going with cybersecurity. The draft guidance indicates FDA’s expectations and requirements for medical device software manufacturers are increasing such that cybersecurity is a critical and ongoing obligation that will impact FDA’s review of pre-market submissions, post-market surveillance, and facility inspections. Although FDA acknowledges that cybersecurity is a shared responsibility among health care facilities, providers, patients, and manufacturers, the Agency expects manufacturers to develop robust cybersecurity protections that will ultimately prevent harm to patients.

National Law Review, Volume VIII, Number 295

Source URL:https://natlawreview.com/article/fda-responds-to-device-software-vulnerabilities-releasing-new-draft-cybersecurity