## **CDRH Releases Postmarket Cybersecurity Final Guidance**

Article By:

Christopher Hanson

On December 28, 2016, CDRH <u>announced</u> the publication of the final guidance<u>"Postmarket</u> <u>Management of Cybersecurity in Medical Devices.</u>" In a <u>separate post</u>, we reported on the January 22, 2016 draft version of this guidance document. The final guidance provides FDA's recommendations on a risk-based framework for medical device manufacturers to assess and remediate cybersecurity vulnerabilities. The guidance also outlines circumstances in which the Agency intends to exercise enforcement discretion with respect to the requirements of 21 C.F.R. Part 806 to report actions related to cybersecurity vulnerabilities as device corrections and removals.

We highlight below key ways the final guidance document differs from the earlier draft version:

- *Applicability of Guidance*. The final guidance clarifies that the document also applies to mobile medical applications, medical devices that are considered part of an "interoperable system," and "legacy devices" (*i.e.*, devices that are already in use or on the market). Furthermore, the guidance explicitly states that the document is not intended to provide guidance on reporting to FDA when a device has or may have caused or contributed to a death or serious injury as required by Section 519 of the Federal Food, Drug, and Cosmetic Act (FDCA) and 21 C.F.R. Part 803 (Medical Device Reporting Regulation).
- *"Patient Harm" Replaces "Essential Clinical Performance."* FDA has deleted the definition of "Essential Clinical Performance" and has instead introduced a definition for "Patient Harm." The Agency states that "Patient Harm" is "physical injury or damage to the health of patients, including death." Instead of framing cybersecurity vulnerabilities as a compromise to essential clinical performance of a device, the final guidance focuses on the risk of patient harm resulting from a vulnerability.
  - The "Patient Harm" definition does not include loss of confidential information, including the compromise of protected health information (PHI). According to the guidance, changes to a device that are made principally to address the loss of confidential information are typically considered to be device enhancements.
  - The Agency does recommend that manufacturers consider protecting the confidentiality of PHI as part of their overall comprehensive risk management program.
- Reporting Actions to Address Cybersecurity Vulnerabilities. As described in the guidance, FDA will not require advance notification or Part 806 reporting when a manufacturer undertakes a "device enhancement" to address cybersecurity vulnerabilities

and exploits. The Agency refers to these actions as "cybersecurity routine updates and patches." For a small subset of actions, FDA will require medical device manufacturers to notify the Agency when such actions "pose a risk to health." The final guidance outlines how to assess whether the risk of patient harm is sufficiently controlled or uncontrolled. Such an analysis is based on an evaluation of: (1) the likelihood of exploit, (2) the impact of exploitation on the device's safety and essential performance, and (3) the severity of patient harm if exploited. In addition, FDA clarifies the circumstances in which FDA does not intend to enforce Part 806 reporting requirements for specific vulnerabilities with uncontrolled risk. FDA will not enforce the requirements when the following are met:

- There are no known serious adverse events or deaths associated with the vulnerability.
- As soon as possible but no later than 30 days after learning of the vulnerability, the manufacturer communicates with its customers and user community regarding the vulnerability, identifies interim compensating controls, and develops a mediation plan. The manufacturer must document the timeline rationale for its remediation plan. The customer communication should, at a minimum: (1) describe the vulnerability including an impact assessment based on the manufacturer's current understanding; (2) state the manufacturer's efforts are underway to address the risk of patient harm as expeditiously as possible; (3) describe compensating controls, if any; and (4) state the manufacturer is working to fix the vulnerability, or provide a defense-in-depth strategy to reduce the probability of exploit and/or severity of harm, and will communicate regarding the availability of a fix in the future.
- As soon as possible but no later than 60 days after learning of the vulnerability, the manufacturer fixes the vulnerability, validates the change, and distributes the deployable fix to its customers and user community, such that the residual risk is brought down to acceptable levels. The manufacturer should follow-up with end-users as needed.
- The manufacturer actively participates as a member of an Information Sharing Analysis Organization (ISAO) and provides the ISAO with any customer communications upon notification of its customers.
- New Cybersecurity Risk Management Program Component. In addition to the critical components of a cybersecurity risk management program outlined in the draft guidance, FDA has added another component, the maintenance of robust software lifecycle processes that include mechanisms for: (1) monitoring third-party software components for new vulnerabilities throughout the device's total product lifecycle, and (2) design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to off-the-shelf software.
- Additional Recommended Vulnerability Assessment Tools. In its draft guidance, FDA recommended that manufacturers consider using a cybersecurity vulnerability assessment tool or similar scoring system for rating vulnerabilities and determining the need for and urgency of the response. FDA noted one such tool, the "Common Vulnerability Scoring System," Version 3.0. In the final guidance, the Agency outlines additional resources that may aid in the triage of vulnerabilities, including AAMI TIR57 and IEC 80001.
- **Disclosure Policy**. The final guidance states that manufacturers should adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of an initial vulnerability report to the vulnerability submitter.
- *"Defense-in-Depth" Strategy for Controlled Risk*. The Agency provides additional examples of vulnerabilities associated with controlled risk and their management, including the development of a "defense-in-depth" strategy. Manufacturers may want to deploy additional controls as part of this strategy, even when risks are controlled. FDA recognizes

that some changes made to strengthen device security might also significantly affect other device functionality, and the manufacturer will want to assess the scope of change to determine if additional premarket or postmarket regulatory actions are appropriate.

"Active Participation in an ISAO." In a new section of the guidance, FDA outlines the criteria the Agency intends to consider in determining whether a manufacturer is an active participant in an ISAO: (1) the manufacturer is a member of an ISAO that shares vulnerabilities and threats that impact medical devices; (2) the ISAO has documented policies pertaining to participant agreements, business processes, operating procedures, and privacy protections; (3) the manufacturer shares vulnerability information with the ISAO, including customer communications pertaining to cybersecurity vulnerabilities; and (4) the manufacturer has documented processes for assessing and responding to vulnerability and threat intelligence information received from the ISAO. FDA recommends that manufacturers maintain objective evidence documenting that these four criteria are met.

© 2025 Covington & Burling LLP

National Law Review, Volume VII, Number 7

Source URL: https://natlawreview.com/article/cdrh-releases-postmarket-cybersecurity-final-guidance