April 14, 2022

FDA Proposes Update to Current Guidance on Cybersecurity in Medical Devices

In response to increasingly frequent and severe cybersecurity threats to the healthcare sector that have the potential to impact clinical outcomes and cause patient harm, the U.S. Food and Drug Administration (FDA) has released draft guidance, applicable to manufacturers of devices automated by software, that would replace guidance released seven years ago.[1] Issued on April 8, the draft guidance emphasizes the need for robust cybersecurity controls to ensure medical device safety and effectiveness as a result of the risks created by the integration of wireless, Internet- and network-connected capabilities, portable media, and electronic exchange of medical device-related information. While FDA guidance does not have the force of law, the FDA's recommendations regarding cybersecurity detailed in this guidance may become binding obligations if they are incorporated into a contract by reference. Additionally, they will establish expectations with respect to premarket submissions and ongoing postmarket programs covering monitoring, servicing, and other actions relating to a connected device. Accordingly, interested parties should understand the principles detailed by the FDA through this draft guidance and consider submitting feedback on the proposal. Comments will be accepted by the FDA until July 7, 2022.

Cybersecurity is part of device safety and the Quality Systems Regulation (QSR) requirements applicable to medical devices in both the premarket and postmarket context, to ensure medical device cybersecurity and maintain device safety and effectiveness. In its draft guidance, the FDA details what it considers to be cybersecurity best practices, such as software validation and risk analyses to demonstrate that a connected device has a reasonable assurance of safety and effectiveness. The FDA also describes what the FDA wants to see in product development by encouraging device makers to implement and adopt a Secure Product Development Framework (SPDF) consisting of a set of processes that would reduce the number and severity of vulnerabilities in products. The draft guidance recommends threat modeling be performed in the design process in order to prevent the need to re-engineer a device when connectivity-based features are added after marketing and distribution, or when vulnerabilities resulting in uncontrolled risks are discovered. It also emphasizes transparency and highlights the importance of manufacturers informing users of cybersecurity controls, potential risks, and other technical information through labeling, such as an operator's manual or security implementation guide, to enable users to manage risks and promptly patch identified issues. Importantly, the FDA notes that inadequate cybersecurity controls may cause a device to be misbranded under the Federal Food, Drug, and Cosmetic Act (FDCA) and implementing regulations because, among other possible violations, its labeling does not bear adequate directions for use or because it is dangerous to health when used in the manner recommend or suggested in the labeling.

The full text of the guidance is linked here: Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff.

---

[1] When final, this guidance will supersede "Content of Premarket Submission for Management of Cybersecurity in Medical Devices-Final Guidance, October 2, 2014."

Authors



Kritika Bharadwaj
Partner

New York, NY | (212) 297-2477

kbharadwaj@daypitney.com



Mindy S. Tompkins
Partner

Hartford, CT | (860) 275-0139

mtompkins@daypitney.com



William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com