JONES DAY

COMMENTARY

MARCH 2019

The FDA and Cybersecurity: How the Agency is Addressing Cybersecurity Risks to Medical Devices

IN SHORT

The Situation: As medical devices become more connected to each other and to the internet, an increasing number of patients are exposed to cybersecurity risks.

The Result: Over the last five years, the Food and Drug Administration ("FDA") has issued new guidance and policy to address cybersecurity issues and has been advised by the Office of Inspector General ("OIG") to take additional steps. Manufacturers should be aware of, and prepare for, the actions FDA undertakes on its own initiative and as a result of the OIG recommendations.

Looking Ahead: Although FDA recognizes that cybersecurity of medical devices is a shared responsibility across the ecosystem, manufacturers of networked medical products have the primary responsibility for managing the cybersecurity risks presented by their products and potentially should be prepared to provide significant cybersecurity information to FDA.

Because of recent and highly publicized data breaches across a multitude of industries, cybersecurity threats have become synonymous with the digital age, and both private and government organizations have invested significant resources into combating the risks presented by digital threats. Although FDA is, to date, unaware of medical devices being hacked or manipulated by unauthorized users while in use by a patient, the threat of such an event is not just theoretical and has received increasing attention from the Agency. Indeed, a number of medical device companies have taken action to address postmarket vulnerabilities that, if exploited, could have allowed an unauthorized user to access a patient's device using commercially available equipment. For example, the FDA has previously issued a safety communication related to a software update to address potential cybersecurity vulnerabilities associated with an implantable device.

FDA's Center for Devices and Radiological Health ("CDRH") is responsible for the oversight of medical devices, including those that are digitally connected to each other or to larger networks, such as the internet. The expanded connectivity of medical devices has led to improvements in patient care and greater efficiencies in the healthcare system (e.g., remote control of devices through mobile apps, as well as faster processing/analyzing of patient data), but also presents new and different types of risks that must be addressed to ensure such products are safe for patient use.

WANT TO KNOW MORE?
Read the full version.

THREE KEY TAKEAWAYS

1. As an ever-greater number of medical devices are connected to the internet, cybersecurity will become an increasingly emphasized aspect of FDA's oversight.

Samir C. Jain
Washington

Colleen M. Heisey
Washington

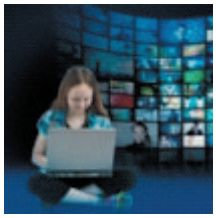
2. FDA has already issued guidance documents that provide cybersecurity recommendations for medical device manufacturers in both the premarket and postmarket contexts.

3. In light of recent OIG reports recommending that FDA take an even greater role in addressing and responding to cybersecurity threats, medical device manufacturers should be prepared to provide FDA with documentation demonstrating that cybersecurity risks have been appropriately managed and mitigated.

J. Todd Kennard
Columbus

Ian M. Pearson
San Francisco

YOU MIGHT BE INTERESTED IN: **Go To All Recommendations >>**



FTC Issues Record Fine for COPPA Violation

Jones Day Global Privacy & Cybersecurity Update | Vol. 21

Jones Day Presents: Smart Contracts and Blockchain

SUBSCRIBE SUBSCRIBE TO RSS

Jones Day is a global law firm with more than 2,500 lawyers on five continents. One Firm Worldwide℠