Thompson & Knight Impact
ATTORNEYS AND COUNSELORS

Client Alert *October 17, 2018*

FDA Releases New Cybersecurity Initiatives for Connected Medical Devices

To kick off National Cybersecurity Awareness Month, the U.S. Food and Drug Administration (FDA) released a statement regarding the agency's continued emphasis on medical device cybersecurity.[1] "The threat of cyber attacks is no longer theoretical," the agency explained. As cyber attacks have become more and more prevalent, the increasing number of medical devices connected to hospital networks creates a greater possibility that cyber criminals could exploit vulnerabilities in medical devices. While the FDA is unaware of any instances of unauthorized users hacking into a medical device, "the risk of such an attack persists."

As part of the agency's continued efforts to bolster medical device cybersecurity, the FDA announced several new initiatives, updates, and collaborations. First, the FDA coordinated with The MITRE Corporation to launch a cybersecurity "playbook" to educate healthcare delivery organizations (HDOs) on the importance of cybersecurity and the impact cyber attacks could have on patients.[2] The playbook provides a primer on medical device cybersecurity; points to preparedness resources available to HDOs; clarifies the roles of HDOs, governments, and medical device manufacturers (MDMs) in the event of a breach; and standardizes the procedure for responding to a cyber attack. Specifically, the playbook outlines a four-tiered approach to any medical device cyber attack: (1) Preparedness; (2) Detection and Analysis; (3) Containment, Eradication, and Recovery; and (4) Post Activity.

The FDA has also entered into two memoranda of understanding in order to create "information sharing analysis organizations," the purpose of which is to create a system by which HDOs, MDMs, and cybersecurity agencies can share information about device vulnerabilities. The hope is that increased transparency across the industry will lead to earlier detection of threats and increased emphasis on patient safety. The FDA is also in the process of executing a memorandum of agreement with the U.S. Department of Homeland Security to further cooperation between government agencies in combating cybersecurity threats related to medical devices.

The FDA's statement also announced its plan to publish "a significant update" to its 2014 guidance document on premarket management of cybersecurity in medical devices.[3] The update will

[1] *See* U.S. Food & Drug Admin., *Statement from FDA Commissioner Scott Gottlieb, M.D., on FDA's efforts to strengthen the agency's medical device cybersecurity program as part of its mission to protect patients* (Oct. 1, 2018), https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm622074.htm.

[2] *See* The MITRE Corporation, *Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook* (Oct. 2018), https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf.

[3] As of October 16, 2018, this update has not been released. The FDA's current premarket guidance document can be found here. Although the FDA did not announce any updates to its postmarket guidance document, that document can be found here.

include recommendations on providing patients with a "cybersecurity bill of materials," which would list the components of any device that could be vulnerable to a cyber attack. This list, the FDA says, should help patients and providers quickly respond to potential threats.

Finally, the FDA's statement highlighted its 2019 budget proposal, which included a request to create a "Center of Excellence for Digital Health." The Center, the statement explained, would work to establish a clearer picture of cybersecurity regulations in the healthcare arena and would house a cybersecurity unit whose task would be to continue researching advances in securing internet-connected medical devices.

These initiatives and updates are proving timely, as states are beginning to consider cybersecurity for Internet of Things devices. Recently, California Governor Jerry Brown signed SB 327 into law, requiring any internet-connected device to have security features to "protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."[4] The law, applying to any product sold or offered for sale in California, is the first state law regulating Internet of Things devices. With the FDA and state governments exploring cybersecurity as it relates to internet-connected devices, it is paramount that healthcare providers use the resources available to them to protect their data and their patients.

If you have any questions, please do not hesitate to contact the Thompson & Knight attorney with whom you regularly work or one of the attorneys listed below.

CONTACTS:

Timothy E. Hudson
214.969.1540
Tim.Hudson@tklaw.com

Mackenzie M. Salenger
214.969.1542
Mackenzie.Salenger@tklaw.com

Connor R. Bourland
214.969.2530
Connor.Bourland@tklaw.com

[4] The full text of the recently passed California law, which will be codified at Title 1.81.26 of Part 4 of Division 3 of the California Civil Code, can be found here.