Thompson & Knight Impact®

ATTORNEYS AND COUNSELORS

Client Alert *January 26, 2016*

FDA's New Guidance on Medical Devices and Cybersecurity Vulnerabilities

The FDA has been scrutinizing cybersecurity risks related to medical devices more closely in recent years. In 2014, the FDA finalized guidelines that focused on cybersecurity threats during the research and development phase of a medical device's lifecycle. On January 22, 2016, the agency expanded its focus and provided draft guidance concerning how medical device makers should monitor, identify, and address cybersecurity vulnerabilities in their devices following their introduction into the marketplace. According to the FDA, this latest guidance is part of its ongoing effort to "ensure the safety and effectiveness of medical devices, at all stages in their lifecycle, in the face of potential cyber threats."[1]

The Federal Food, Drug, and Cosmetic Act (the "Act") requires device manufacturers to report to the FDA certain actions concerning device corrections and removals within ten working days of initiation.[2] According to the new draft guidance, however, the agency "does not intend to enforce certain reporting requirements of the Act against companies" that "voluntarily participate in [an Information Sharing Analysis Organization ("ISAO")]" and follow its other recommendations.[3]

For example, "cybersecurity vulnerabilities and exploits that may compromise the essential clinical performance of a device and present a reasonable probability of serious adverse health consequences or death" would trigger the Act's prompt reporting provision. But the draft guidance indicates that in cases where the vulnerability is quickly addressed in a way that sufficiently reduces the risk of harm to patients, the FDA does not intend to enforce urgent reporting of the vulnerability to the agency if the following conditions are met:

- There are no known serious adverse events or deaths associated with the vulnerability;
- Within 30 days of learning of the vulnerability, the manufacturer identifies and implements device changes and/or compensating controls to bring the residual risk to an acceptable level and notifies users; and
- The manufacturer is a participating member of an ISAO, such as NH-ISAC.[4]

[1] The FDA's draft guidance, *Postmarket Management of Cybersecurity in Medical Devices*, is available at the following link: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

[2] As discussed more fully below, the FDA will consider most—but certainly not all—actions taken by manufacturers to address cybersecurity vulnerabilities to be "cybersecurity routine updates or patches," which manufacturers may simply disclose in an annual report.

[3] Congress has defined the term "Information Sharing and Analysis Organization" as any formal or informal entity or collaboration created by public or private sector organizations for the purpose of gathering and analyzing information to better understand security problems. 6 U.S.C. § 131(5).

[4] The National Health Information Sharing and Analysis Center, or NH-ISAC, seeks to "enable and preserve the public trust by advancing health sector cybersecurity protection and the ability to prepare for and respond to threats and vulnerabilities." *See* NH-ISAC, http://www.nhisac.org/faq/#Q1 (last visited Jan. 22, 2016).

The main purpose of the new draft guidance is to urge medical device makers to "implement . . . comprehensive cybersecurity risk management program[s]." Device makers retain discretion concerning the design of such programs under the draft guidance. But the FDA suggests that the following components are "critical":

- Applying the 2014 NIST voluntary Framework for Improving Critical Infrastructure Cybersecurity, which includes the core principles of "Identify, Protect, Detect, Respond, and Recover;"[5]
- Participating in an ISAO;
- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Understanding, assessing, and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond, and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation.

All told, the FDA's newest draft guidance strongly encourages medical device manufacturers to take a proactive and collaborative approach to cybersecurity management of their medical devices. Interested parties may comment on the draft guidelines until April 21, 2016.

If you have additional 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

Michael C. Titens
214.969.1437
Michael.Titens@tklaw.com

Susan B. Murphy
713.653.8677
Susan.Murphy@tklaw.com

Alexander Dimock
214.969.1155
Alex.Dimock@tklaw.com

[5] The Framework for Improving Critical Infrastructure Cybersecurity is available at the following link: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.