FEBRUARY 24, 2020

For more information, contact:

Adam Solander
+1 202 626 5542
asolander@kslaw.com

Lisa Dwyer
+1 202 626 2393
ldwyer@kslaw.com

Michael Dohmann
+1 202 626 9263
mdohmann@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

FDA FY 2021 Budget Foretells Medical Device Cybersecurity Reform

Increased premarket submission and post-market reporting requirements potentially on the horizon for high-tech devices.

The Food and Drug Administration's ("FDA's") budget proposal for FY2021 telegraphs FDA's plan to seek new legislative authority to compel medical device manufacturers to address cybersecurity risks.

Specifically, FDA seeks new authority that would allow the Agency to require that: (1) devices have the capability to be updated and patched in a timely manner; (2) premarket submissions to FDA include evidence demonstrating the capability from a design and architecture perspective for device updating and patching; (3) device manufacturers provide a Cybersecurity Bill of Materials; and (4) device manufacturers publicly disclose any new information about a cybersecurity vulnerability that arises post-market, to alert users that a device may be vulnerable and to provide direction to users to reduce their risk. FDA is also seeking new authority to improve proactive responses to cybersecurity vulnerabilities (although FDA's proposal does not explain what the triggers for the proactive responses would be, or what the proactive responses may look like).

The new legislative requirements would supplement the requirements currently imposed by the Quality System Regulation ("QSR") and/or effectively codify recommendations that FDA has already issued through guidance. Significantly, the QSR already requires device manufacturers to establish and maintain procedures for validating a device's design, including establishing and maintaining software validation procedures and *risk analysis* procedures. The QSR also already requires device manufacturers to establish and maintain procedures for complaint handling, quality audits, corrective and preventive action, and servicing. Notably, FDA has issued a guidance entitled "Postmarket Management of

Cybersecurity in Medical Devices," which makes clear that cybersecurity risk management programs that are consistent with the QSR *should* address vulnerabilities that may permit unauthorized access to information stored on, or transferred by, a device. To that end, FDA recommends that manufacturers develop post-market surveillance programs that allow the manufacturer to identify vulnerabilities, assess their impact, and assess the severity of the potential patient harm.

In addition, FDA has issued two guidances with recommendations regarding the type of cybersecurity information that device manufacturers *should* submit to FDA in premarket submissions. In 2014, FDA issued a short, 7-page, final guidance on this topic entitled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." That guidance stated that device manufacturers *should* establish design inputs for their devices related to cybersecurity, and establish a cybersecurity vulnerability and management approach, as part of their obligations under the QSR. According to FDA, that approach should address: (1) identification of assets, threats, and vulnerabilities; (2) assessment of the impact of threats and vulnerabilities on device functionality and end users/patients; (3) assessment of the likelihood of a threat and of a vulnerability being exploited; (4) determination of risk levels and suitable mitigation strategies; and (5) assessment of residual risk and risk acceptance criteria. Further, that guidance recommended that device manufacturers submit certain information in their pre-market submissions to show that their QSR requirements were being met, including a "summary describing the *plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device to continue to assure its safety and effectiveness*."

Although the 2014 guidance is still in effect, FDA issued a ***draft*** guidance in 2018, with the same name— "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." If that guidance is finalized, it will supersede the 2014 guidance. The 2018 draft guidance is much more detailed than the 2014 guidance, and stands at 24 pages, compared to 7. Among other things, the 2018 draft guidance recommends that medical device manufacturers provide information in premarket submissions that includes a "*summary describing the design features that permit validated software updates and patches as needed throughout the lifecycle of the device*." Notably, the 2018 draft guidance also recommends that the labeling for devices include a *Cybersecurity Bill of Materials, with "a list of … software and hardware components to enable device users … to effectively manage their assets, to understand the potential impact of identified vulnerabilities to the device (and the connected system), and to deploy countermeasures to maintain the device's essential performance*."

Not surprisingly, FDA's legislative proposal—which would *require* that devices have the capability to be updated and patched in a timely manner, that premarket submissions to FDA include evidence demonstrating that capability, and that device manufacturers submit a Cybersecurity Bill of Materials—largely tracks the recommendations in FDA's guidance. The advantage of legislation to FDA is that if its recommendations were effectively codified in statute, they would become enforceable legal obligations.

But, a prescriptive legislative approach may not be practical for device manufacturers. For example, device manufacturers may not be able to show that their devices are capable of remotely patching cybersecurity issues. Meeting that requirement would not be technically feasible if device manufacturers do not have expansive post-market access to their products. Furthermore, creating a remote patching capability may introduce additional attack vectors to a device where the harm of the potential remote exploitation may outweigh the security risk. The non-prescriptive approach in the guidance has allowed the industry to take a risk-based approach and to implement the recommendations in the guidance that make sense for a particular product.

Moreover, the novel provisions in the legislation—which would require public disclosure of cybersecurity vulnerabilities that arise postmarket, as well as proactive responses to those vulnerabilities—may not always advance FDA's interest of better protecting the public health. For example, in certain circumstances, disclosing vulnerabilities could, ironically, decrease cybersecurity by alerting hackers to opportunity.

Given the potentially significant implications of the type of legislation that FDA is proposing, King & Spalding recommends that medical device manufacturers follow developments closely and engage with FDA and Congress, if necessary. King & Spalding would be happy to assist manufacturers in that regard.