Client Update

FDA Publishes Guidance on Postmarket Cybersecurity Risk Management for Medical Device Manufacturers

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Mark P. Goodman
mpgoodman@debevoise.com

Maura Kathleen Monaghan
mkmonaghan@debevoise.com

Jim Pastore
jjpastore@debevoise.com

David Sarratt
dsarratt@debevoise.com

Jacob W. Stahl
jwstahl@debevoise.com

Jonathan Metallo
jmetallo@debevoise.com

As the "Internet of Things" grows, the digital target for malicious actors is growing with it. Not long ago, researchers at the University of South Alabama reported the results of an exercise which confirmed that "a student with basic information technology and computer science background" could hack medical devices such as a pacemaker, defibrillator, or insulin pump, with devastating effects on the patient. In the wake of this and similar warnings, the FDA issued "Postmarket Management of Cybersecurity in Medical Devices" (the "Postmarket Guidance").

While the Guidance is technically nonbinding and has not yet been finalized, it indicates that the failure to address cybersecurity vulnerabilities may be deemed a violation of the Food, Drug, and Cosmetic Act ("FDCA"). The guidance is directed to device manufacturers, but also emphasizes that securing devices is the responsibility of other stakeholders including health care facilities, providers, and patients.

GENERAL PRINCIPLES OF EFFECTIVE CYBERSECURITY MANAGEMENT

The FDA has joined other regulators in encouraging the adoption of the NIST Framework for Improving Critical Infrastructure Cybersecurity (the "NIST Framework") with its key principles of Identify, Detect, Protect, Respond and Recover. The NIST Framework serves as guide for "critical infrastructure organizations" to effectively protect themselves from cybersecurity threats. It has quickly gained traction in the private sector, in critical and noncritical industries alike.

Additionally, the FDA encourages stakeholders to participate in Information Sharing Analysis Organizations ("ISAOs") to share and disseminate information on cybersecurity vulnerabilities and exploits. Recognizing the importance for businesses to collaborate on cybersecurity intelligence, the FDA "strongly

recommend[s]" joining an ISAO. The FDA tacitly endorses one ISAO by highlighting its own connection to the National Health Information Sharing & Analysis Center ("NH-ISAC").

SPECIFIC GUIDANCE ON SECURING MEDICAL DEVICES

The FDA describes in great detail how it expects manufacturers will identify, assess, and respond to cybersecurity vulnerabilities. This description provides insight for all healthcare stakeholders on the cybersecurity standard of care the FDA is establishing.

The FDA sets forth a framework focused on maintaining the "essential clinical performance" of medical devices, a term manufacturers should define with respect to individual devices. Manufacturers should work with others in the healthcare industry to identify device vulnerabilities and assess the risk posed to essential clinical performance.

The level of risk posed by a vulnerability will depend on an evaluation of (a) the difficulty of exploiting it and (b) the severity of the potential health impact that would follow. Notably, the FDA offers specific suggestions on the means for this evaluation:

- To evaluate a vulnerability's exploitability, the FDA cites the "Common Vulnerability Scoring System," issued by the Forum of Incident Response and Security Teams (known as "FIRST"), as a useful tool for assessing the exploitability of vulnerabilities.
- To evaluate the severity of a vulnerability's potential health impact, the FDA recommends guidance from ISO entitled "Medical devices – Application of risk management to medical devices."

This reflects a growing trend among regulators to be quite prescriptive on cybersecurity. For example, the New York Department of Financial Services communicated with a number of federal regulators late last year on the need for specific cybersecurity regulations in the financial services sector, suggesting mandates for the appointment of a Chief Information Security Officer and the implementation of multi-factor authentication.

The FDA expects manufacturers to use such tools to assess vulnerabilities as presenting a "low," or controlled risk to a device's essential clinical performance, or a significant, "uncontrolled risk." Certain expectations come with these risk categories:

Controlled Risks: If the manufacturer determines risks are controlled, any changes that it makes to medical devices – such as routine updates and patches – to address identified risks do not need to be reported to the FDA. Routine changes must be disclosed, however, as part of periodic reports that are submitted for Class III devices.

Uncontrolled Risks: If the manufacturer determines risks are uncontrolled, the risks and remediation should be reported to the FDA under 21 C.F.R. 806.10. However, the FDA indicates that it will not require reporting under this regulation when: (a) no serious adverse events or deaths are known to be associated with the vulnerability; (b) within 30 days of learning of the vulnerability, the manufacturer implements changes to mitigate risk; and (c) the manufacturer is a member of an ISAO, such as NH-ISAC.

Regardless of whether manufacturers inform the FDA of an uncontrolled risk, the FDA expects manufacturers to inform the user community about temporary fixes for any vulnerability until the problem is remediated. Further, if a manufacturer fails to address uncontrolled risks to its device's essential clinical performance, the FDA will assess the risk posed to patient health in evaluating whether a violation of the FDCA has occurred.

IMPACT OF THE POSTMARKET GUIDANCE

With the Postmarket Guidance, the FDA takes direct aim at imposing standards on medical device manufacturers, but it is a safe bet that neither the FDA nor other regulators will stop there. The Guidance itself emphasizes the shared responsibility of all healthcare stakeholders to address cybersecurity on an ongoing basis. Adopting the NIST Framework and participating in ISAOs seem wise steps for any business subject to FDA scrutiny. Going forward, other regulators, the plaintiffs' bar and courts may also point to the FDA guidance as contributing to an emerging standard of care that could, in time, support legal liability under various theories.

Anyone can provide feedback on the draft Guidance within 90 days of January 15, either in writing to the FDA, or online via http://www.regulations.gov.

* * *

Please do not hesitate to contact us with any questions.