Hogan Lovells

FDA signals increasing focus on cybersecurity requirements

25 April 2018

With the continued explosion of software and software-controlled medical devices, including the growing use of machine learning and artificial intelligence, the FDA (the Agency) Medical Device Safety Action Plan (the Plan) released last week[1] highlights the Agency's increasing focus on cybersecurity. In announcing the plan, FDA Commissioner Scott Gottlieb emphasized the importance of cybersecurity in ensuring patient safety. The Plan recognizes that the increased interconnectedness of medical devices of all types can lead to safer, more effective technologies, but also introduces increased potential for security breaches and exploitation of device vulnerabilities. While progress has been made in this area, the Agency maintains that additional efforts are needed to prevent, detect, and respond to threats such as hacking and cyber attacks. Accordingly, the Agency's fiscal year (FY) 2019 budget request asks for authority and appropriations to impose new obligations on device manufacturers, as well as to enhance FDA's ability to assess these issues as they arise.[2]

Pre-market endeavors

FDA may ask Congress to grant it the authority to require medical device manufacturers to incorporate cybersecurity into their products, including ensuring that the design enables timely patching and updates where needed. Congress has been actively considering similar issues in connection with legacy technologies, with the House Energy and Commerce Committee recently issuing a request for information regarding patching, updates, and vulnerability management.[3] Under FDA's new Safety Action Plan, medical device pre-market submissions (including 510(k)s, De Novos, and PMAs) would also be required to include:

- A Software Bill of Materials that would be made available to customers and users to help better manage networked assets and raise awareness of potential vulnerabilities; and
- Adequate data regarding cybersecurity, such that FDA can appropriately assess this capability as part of the pre-market review process.

In addition, FDA intends to update its pre-market guidance on medical device cybersecurity[4] to better protect against both moderate risks (i.e., those that could disrupt clinical operations and/or delay patient care) and major risks (i.e., those that exploit a vulnerability to enable a

[1] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm604672.htm.
[2] https://www.fda.gov/downloads/AboutFDA/ReportsManualsForms/Reports/BudgetReports/UCM603315.pdf
[3] https://energycommerce.house.gov/wp-content/uploads/2018/04/20180420Supported_Lifetimes_RFI.pdf.
[4] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

remote, multi-patient, catastrophic attack). This appears to be in part a reaction to the significant ransomware cyberattacks that occurred in 2017 involving WannaCry and Petya/NotPetya.

Post-market endeavors

In the post-market sphere, FDA will consider requiring firms to adopt policies and procedures for coordinated disclosure of cybersecurity vulnerabilities as they are identified. This would supplement the expectations set forth in FDA's existing guidance documents, Postmarket Management of Cybersecurity in Medical Devices (Dec. 2016)[5] and Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (May 2005)[6], adherence to which is strongly recommended but not legally binding.

In conjunction, the Agency has proposed the development of a CyberMed Safety (Expert) Analysis Board (CYMSAB) to complement existing resources for device firms and FDA, and address the unmet need for a holistic, multi-disciplinary approach in this area. The CYMSAB would be a public-private partnership comprised of individuals from government, private industry, and academia with a broad range of expertise—including not just networking and software, but also clinical affairs, biomedical engineering, and other fields—to assess and validate high-risk/high-impact device vulnerabilities and incidents while taking into account patient safety and clinical environments. The new board would also adjudicate disputes, assess proposed mitigations, advise entities on how to properly disclose vulnerabilities under the new requirements intended to be established, and investigate suspected or confirmed device compromises at the request of either a manufacturer or FDA. This may be a further development of a more informal response team approach that FDA has been using over the past year or so. Creation of the CYMSAB would be funded using part of the $70 million included in FDA's budget request for the creation of a Center of Excellence on Digital Health.

Conclusion

While FDA already has broad authority to impose heightened premarket and post-market requirements on medical devices to address cybersecurity threats, FDA believes the proposed additions to its digital health regulatory framework will help mitigate the occurrence and severity of cyber threats, as well as streamline post-market mitigations. In addition to the cybersecurity space, FDA has also requested new funding and authority across the Center for Devices and Radiological Health's (CDRH's) jurisdiction, including for initiatives that may not require additional Congressional authorization—such as enhanced evaluation of real-world data and roll-out of the software pre-certification program (see our prior client alerts[7]). The FY2019 request seeks $5.8 billion for FDA as a whole; of this, $635,635 is for the CDRH, representing an increase of 26 percent ($130,791) over the Center's allocation in FY2018. It remains to be seen whether Congress will agree to provide the requested additional authority and funding, and whether this will lead to promulgation of cybersecurity-specific regulations to make the associated responsibilities legally enforceable on device firms.

[5] https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ UCM482022.pdf
[6] https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ UCM077823.pdf
[7] https://www.hoganlovells.com/en/publications/fdas-software-pre-cert-program-more-details-revealed; https://www.hoganlovells.com/en/publications/fda-unveils-software-pre-certification-pilot-program-to-foster-digital-health-innovation

Contacts

Jodi Scott
Partner, Denver
T +1 303 454 2463
jodi.scott@hoganlovells.com

Yarmela Pavlovic
Partner, San Francisco
T +1 415 374 2336
yarmela.pavlovic@hoganlovells.com

Paul Otto
Senior Associate, Washington, D.C.
T +1 202 637 5887
paul.otto@hoganlovells.com

Suzanne Levy Friedman
Associate, Washington, D.C.
T +1 202 637 5532
suzanne.friedman@hoganlovells.com

www.hoganlovells.com