Hogan Lovells

Proposed changes to FDA guidance for the content of premarket submissions for management of cybersecurity in medical devices: What you should know

October 19, 2018

October is National Cybersecurity Awareness Month and the Food and Drug Administration (FDA or the agency) has been busy. On October 18, 2018, FDA issued a long-awaited draft revision to its existing guidance "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (premarket cybersecurity guidance). This coincided with the release of the FDA-supported "Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook" for health delivery organizations (HDOs), the announcement of two new Information Sharing Analysis Organizations (ISAOs), and FDA's recent news release discussing the agency's enhanced cybersecurity partnership with the U.S. Department of Homeland Security (DHS) earlier this month. Consistent with the U.S. Department of Health and Human Services - Office of Inspector General's September 2018 report "FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices," FDA's recent flurry of activity focuses on providing additional clarity about when to interact with FDA, what information would be useful in submissions, and what level of documentation is expected. Cybersecurity clearly is a high priority issue for FDA and the agency is working hard to bring together stakeholders and provide the best information it can so that all entities that are involved in managing the multifaceted and evolving area of cybersecurity have the best and most current information to manage the risks of a cybersecurity intrusion.

This alert explains the following:

- what is changing with the premarket cybersecurity guidance
- the significance of the new HDO playbook
- what the new ISAOs and partnership between the FDA and the DHS mean for you

Key updates to FDA's premarket cybersecurity guidance

On October 18, 2018, FDA issued its revised draft premarket cybersecurity guidance. When final, the new guidance will supersede the final October 2, 2014 guidance of the same name. Like its predecessor, the updated guidance addresses the recommended content and information to be included in premarket submissions to address cybersecurity risks for impacted devices, and

stresses FDA's view that medical device security is a shared responsibility among all stakeholders, including health care facilities, patients, health care providers, and manufacturers of medical devices. Cybersecurity recommendations for devices that have already received clearance or approval from FDA are provided in FDA's guidance: "Postmarket Management of Cybersecurity in Medical Devices" (postmarket cybersecurity guidance).

The new draft premarket cybersecurity guidance provides information designed to aid manufacturers in determining how to meet the agency's expectations during premarket review of medical devices. The guidance first addresses design and development of devices by encouraging manufacturers to (1) employ a risk-based approach in the design and development of a medical device, (2) take a holistic approach by assessing risk and mitigations throughout the product life cycle, (3) ensure maintenance and continuity of critical device safety and essential performance, and (4) promote the development of trustworthy devices to ensure continued safety and effectiveness. The key features of the agency's new guidance are described below.

- **Risk-based design, validation, and the CBOM.** As a guiding principle, FDA emphasizes the need for device design to address the intended uses of the device and the needs of the user, including cybersecurity, as well as the need to conduct thorough software validation and risk assessment, as required by the quality system regulation (QSR)(21 CFR Part 820). Manufacturers are encouraged to employ a risk-based approach in determining the design features and level of cybersecurity resilience appropriate for each specific device, and to employ a cybersecurity bill of materials (CBOM) to be shared with customers to identify assets, threats, and liabilities. Any CBOM should include but is not necessarily limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities. Although the idea of requiring manufacturers to provide a CBOM (or more generally a software bill of materials, or SBOM) to their customers has been floated and discussed by FDA for some time (including during the FDA's 2017 cybersecurity workshop and in the FDA's 2018 "Medical Device Safety Action Plan"), it has not been embraced by the industry. This is the first time that FDA has been clear as to its expectation that it be created by manufacturers and provided to customers.

- **Tiers of risk.** The guidance introduces two tiers of devices based on their cybersecurity risk levels. These risk tiers are then used to define categories of design requirements and supporting documentation that should be submitted to FDA in a marketing application. Specifically:

  - Tier 1 "Higher Cybersecurity Risk": A device is a Tier 1 device if (1) the device is capable of connecting to another medical or non-medical product, to a network, or to the internet **and** (2) a cybersecurity incident affecting the device could directly result in patient harm to multiple patients.

  - Tier 2 "Standard Cybersecurity Risk": A medical device for which criteria for a Tier 1 device are not met, in other words, everything else.

  Examples of Tier 1 devices include implantable cardioverter defibrillators (ICDs), pacemakers, neurostimulators, dialysis devices, and infusion and insulin pumps, among others. The guidance clarifies that these tiers are not linked to device classification, but are intended to be broadly applicable to all medical devices.

  FDA also provided a definition of "patient harm" for purposes of this guidance, which is defined as "physical injury or damage to the health of patients, including death. Cybersecurity exploits (e.g., loss of authenticity, availability, integrity, or confidentiality) of a device may pose a risk to health and may result in patient harm." FDA also clarified that although

manufacturers are obligated to protect the confidentiality, integrity, and availability of protected health information (PHI) throughout the product life cycle under other legal authorities, for purposes of FDA's regulations, the agency does not consider other harms, such as loss of confidential PHI, to fall within the "patient harms" discussed in the draft guidance. Generally speaking, the measures recommended by FDA are intended to reduce the risk of multi-patient harm, in particular due to the loss of authenticity, availability, integrity, and confidentiality.

- **The trustworthy device.** The draft guidance also introduces the concept of a "trustworthy" device, which is defined in the draft guidance as one that (1) is reasonably secure from cybersecurity intrusion and misuse; (2) provides a reasonable level of availability, reliability, and correct operation; (3) is reasonably suited to performing its intended functions; and (4) adheres to generally accepted security procedures.

- **Application of the design considerations.** The draft guidance expands upon the specific design features and cybersecurity controls that the agency believes should be included in the design of a trustworthy device by including explicit reference to the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Namely, (1) Identify; (2) Protect; (3) Detect; (4) Respond; and (5) Recover. While many of these concepts were covered in the previous version of this guidance, the draft premarket cybersecurity guidance provides additional detail regarding specific considerations and methods to address each of these elements. Importantly, premarket submissions for Tier 1 devices are expected to include documentation of how the device design and risk assessment incorporate each of the controls described in the guidance, while submissions for Tier 2 devices may provide a combination of this type of documentation and rationales explaining why certain controls are not appropriate for the device. Detailed risk assessments along with traceability to implemented measures and testing should also be provided.

- **Cybersecurity labeling documentation.** The draft guidance provides new recommendations for complying with FDA's labeling regulations, as well as communicating relevant security information to end users to ensure a device remains safe and effective throughout its complete life cycle, even during instances where cybersecurity may have been compromised. The labeling should provide users with sufficient information that facilitates the development of risk management plans at the customer site. Key to this aspect is the creation and provision of a CBOM, as discussed above.

- **Cybersecurity documentation.** The draft guidance extends the 2014 guidance recommendations for cybersecurity documentation to be provided in medical device submissions. However, software manufacturers that design their device in-line with the FDA guidance "General Principles of Software Validation; Final Guidance for Industry and FDA Staff" and "AAMI TIR57: Principles for medical device security –Risk management," should not find themselves in unfamiliar territory.

The partnership between FDA and the DHS

In parallel with the release of the draft guidance, FDA issued a news release announcing a new memorandum of agreement between the FDA's Center for Devices and Radiological Health (CDRH) and U.S. Department of Homeland Security's (DHS) Office for Cybersecurity and Communications. Although the two agencies already work together on many aspects of medical device cybersecurity, the new agreement is meant to encourage even greater coordination and information sharing about potential or confirmed medical device cybersecurity vulnerabilities and threats.

The memorandum addresses the following:

- **Vulnerability coordination.** The DHS will continue to serve as the central medical device vulnerability coordination center and interface with the appropriate stakeholders.
- **Risks to patient health and potential for harm.** FDA will continue to engage in regular, ad hoc, and emergency calls, and continue to advise the DHS on risks to patient health and potential for harm.

Execution of this memorandum of agreement (MOA) formalizes existing relationships and close ties between FDA and the DHS, thereby further strengthening the relationship and collaboration. Ideally, the MOA will also provide a foundation for quick coordination and reaction when the next major vulnerability comes to light. We also note that FDA has supported a recent Medical Device Innovation Consortium (MDIC) white paper as an approach to help with coordinated vulnerability disclosures.

The significance of the new HDO playbook

Amid these other efforts focused on enhanced cybersecurity guidance aimed at manufacturers, FDA also sponsored new guidance to help health delivery organizations (HDOs) better understand and prepare for potential incidents involving medical devices. With FDA's support and input, on October 1, 2018, the MITRE Corp. (a federally funded non-profit research organization) released a new HDO playbook addressing cybersecurity incidents involving HDO's medical devices. The widespread ransomware attacks affecting HDOs worldwide in 2017, such as WannaCry and Petya/NotPetya, served as a wake-up call for the agency to help push out more detailed guidance to help the health sector better prepare for and respond to such events in the future.

The playbook walks through the various steps for preparedness and response to such incidents, with a focus on how HDOs manage the process and interact with other stakeholders throughout the life cycle of an incident. The goal is to support regional incident preparedness and response activities to help limit the potential impact on patient care and safety when a cybersecurity incident occurs. While FDA emphasizes that the playbook is a key resource for emergency/incident preparedness and response, it is not intended to be viewed as a stand-alone document to be reviewed in isolation. Rather, the playbook picks up where manufacturers' obligations end and the responsibility of managing cybersecurity risk picks up at the HDO's facility. The playbook assumes that information about the cybersecurity risk in products is provided by the manufacturer and the HDO is able to then take that information and build a cybersecurity risk management plan, thereby creating a mechanism of continuous cybersecurity risk management from the product's development into the use environment.

Creation of Two New ISAOs

In addition, on October 1, 2018, FDA announced two memoranda of understanding to support creation of new ISAOs: MedISAO and Sensato-ISAO. These ISAOs provide further opportunities for manufacturers to share information about emerging threats and potential vulnerabilities. The FDA encourages participation in the ISAOs through several means, including the FDA's postmarket cybersecurity guidance—where active participation in an ISAO is one factor in support of a manufacturer avoiding a reportable recall. Because cybersecurity is an area with responsibility distributed across various stakeholders, each with a common goal, communication among the stakeholders is one of the core components of managing the risk and, as a result, FDA is hard at work to facilitate open communication channels and clarify roles. That said, FDA clearly expects manufacturers to do their part to lay the foundation by designing cybersecurity

controls into products and informing users of potential areas of risk so that health care facilities have the information they need to manage their own cybersecurity risk in the greater ecosystem.

Conclusion

The efforts described above are part of FDA's continuing focus on cybersecurity and its drive to improve the cybersecurity infrastructure in the medical device industry and push a coordinated approach throughout the health care system. In keeping with the approach outlined in the agency's new draft guidance, we have seen a considerable escalation in the focus and detailed nature of FDA's cybersecurity review during the premarket phase. Recent reviews have included very detailed questions regarding choices made by the manufacturer, including, in some instances, requests to modify the device in specific ways. As the agency becomes more knowledgeable of the risks and mechanisms to manage those risks, we expect to see continued action from the agency as well as its partners to increase awareness and drive comprehensive planning around the risk.

FDA plans to hold a two day meeting on January 29–30, 2019 to discuss the draft guidance. FDA is also seeking stakeholder comments on the proposals in the guidance, particularly with regard to the extent and format of a CBOM. All comments are due by March 18, 2019.

Contacts

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

Randy J. Prebula
Partner, Washington, D.C.
T +1 202 637 6548
randy.prebula@hoganlovells.com

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

Danielle C. Humphrey
Counsel, Washington, D.C.
T +1 202 637 8853
danielle.humphrey@hoganlovells.com

Lina R. Kontos
Counsel, Washington, D.C.
T +1 202 637 5713
lina.kontos@hoganlovells.com

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

W. Alex Smith
Directory of Regulatory Sciences, Washington, D.C.
T +1 202 637 5697
alex.smith@hoganlovells.com