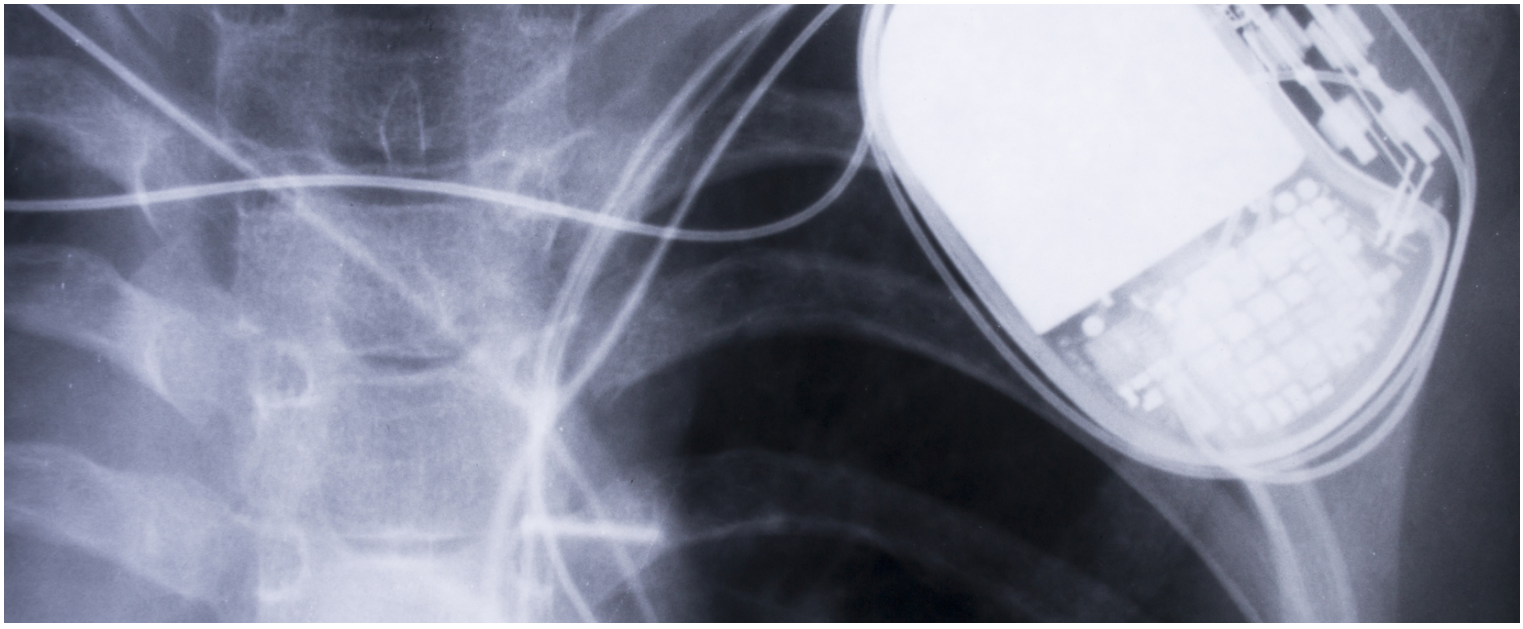
Feb 2019

USA: Staying secure - FDA's evolving approach to medical device cybersecurity

As the introduction of new medical devices continues to become a major part of the US healthcare sector, the mitigation of cybersecurity risks to such devices is an area of increasing focus for the U.S. Food and Drug Administration ('FDA'). Given the rate of technological advancement, the FDA has had to be equally fast-moving in developing its approach to medical device review processes and the issuance of new guidance. Yarmela Pavlovic and Shilpa Prem, of Hogan Lovells, discuss the major initiatives taken by the FDA in the last year to expand the knowledge base, and to provide stakeholders the information they need to increase the cybersecurity of their medical devices.



Fodor90/Signature collection/istockphoto.com

In the past decade, cybersecurity has evolved from an almost non-existent issue to possibly the most critical issue for medical technology. Working to keep pace with technological evolution, the FDA's approach to cybersecurity has also rapidly evolved, and is one of the key areas of focus in its 2019 plans. The FDA's recent efforts respond to both significant advancements in technology, as well as high profile examples of potential cybersecurity vulnerabilities. Kicking off the year with a workshop on premarket cybersecurity issues[1], the FDA aims to build on work over the last few years to develop a comprehensive set of guidance documents to aid manufacturers in navigating their cybersecurity approach.

Updated premarket cybersecurity guidance

On 18 October 2018, the FDA issued a revised draft premarket cybersecurity guidance, titled Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff ('the Premarket Guidance'). When final, the Premarket Guidance will supersede the 2 October 2014 guidance of the same name. As with the prior version, the updated Premarket Guidance describes the recommended content for premarket submissions to address cybersecurity risk and associated mitigation strategies. The Premarket Guidance also stresses the FDA's view that medical device security is a shared responsibility among all stakeholders, including healthcare facilities, patients, healthcare providers, and manufacturers of medical devices.

The Premarket Guidance encourages manufacturers to:

- employ a risk-based approach in the design and development of a medical device;
- take a holistic approach by assessing risk and mitigations throughout the product life cycle;
- ensure maintenance and continuity of critical device safety and essential performance; and
- promote the development of trustworthy devices to ensure continued safety and effectiveness.

The key features of the Premarket Guidance are as follows:

Risk-based design, validation, and the CBOM

As a general principle in medical device development and manufacturing, in order to demonstrate that the device is safe and effective, a manufacturer must establish and maintain procedures for validating the device design which shall include software validation and risk analysis, where appropriate[2]. As part of the software validation and risk analysis, software device manufacturers may need to establish a cybersecurity vulnerability assessment. The FDA emphasises that medical devices that are capable of connecting (wirelessly or hard-wired) to another device, to the internet or other network, or to portable media (e.g., USB or CD) are more vulnerable to cybersecurity threats than devices that are not connected. The Premarket Guidance encourages manufacturers 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. The CBOM identifies the assets, threats, and liabilities of the product, and provides a list of software and hardware components of a device that could be susceptible to vulnerabilities. This is the first time that the FDA has specifically outlined plans to require a CBOM.

Tiers of risk

The Premarket Guidance introduced two tiers of devices based on their cybersecurity risk levels. It proposes requiring different sets of documentation in a marketing application based on the cybersecurity tier level of the device. The Premarket Guidance clarifies that these tiers are not linked to device classification, but are intended to be broadly applicable to all medical devices. The tiers of devices are as follows:

Tier 1 'Higher Cybersecurity Risk'
A medical device is a Tier 1 device if:

- the device is capable of connecting to another medical or non-medical product, to a network, or to the internet; and
- a cybersecurity incident affecting the device could directly result in patient harm to multiple patients.

Examples of Tier 1 devices include implantable cardioverter defibrillators (ICDs), pacemakers, left ventricular assist devices (LVADs), brain stimulators and neurostimulators, dialysis devices, infusion and insulin pumps, and the supporting connected systems that interact with these devices such as home monitors and those with command and control functionality such as programmers.

Tier 2 'Standard Cybersecurity Risk'
A medical device is a Tier 2 device if the criteria for a Tier 1 device are not met.

The trustworthy device

A major theme of the Premarket Guidance is encouraging manufacturers to design devices that are 'trustworthy,' because trustworthy devices are more likely to remain safe and effective throughout their lifecycle. The Premarket Guidance defines a 'trustworthy' device as a device that:

- is reasonably secure from cybersecurity intrusion and misuse;
- provides a reasonable level of availability, reliability, and correct operation;
- is reasonably suited to performing its intended functions; and
- adheres to generally accepted security procedures.

Cybersecurity labelling

The Premarket Guidance explains the role of labelling with respect to the safety and effectiveness of devices with cybersecurity risks. Specifically, the FDA emphasises that end-users be informed of security information through labelling to help mitigate cybersecurity risks and help ensure the continued safety and effectiveness of the device. Furthermore, the FDA recommends specific security information be included in the labelling, such as the use of anti-virus software, use of a firewall, a description of backup and restore features, and procedures to regain configurations after the device's cybersecurity has been compromised, etc.

MOA between the FDA and the DHS

Also in the fall of 2018, the FDA's Center for Devices and Radiological Health ('CDRH') and the U.S. Department of Homeland Security ('DHS') Office for Cybersecurity and Communications entered into an Memorandum of Agreement ('MOA'). Although the two agencies have already worked together on many aspects of medical device cybersecurity, the MOA provides a framework for increased coordination and collaboration.

The MOA was executed to formalise and enhance the working relationship of the two agencies, including roles and responsibilities when sharing information related to vulnerabilities and threats related to the public health that involve the cybersecurity of medical devices. Under the MOA, the DHS continues to serve as the central medical device vulnerability coordination centre and interfaces with appropriate stakeholders in performance of such duties. The FDA continues to coordinate and participate in regular ad hoc and emergency coordination calls with the DHS to enhance mutual awareness of medical device vulnerabilities and threats to the healthcare and public sector.

The Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook

In addition to efforts focused on enhancing cybersecurity guidance for medical device manufacturers, the FDA has also worked with a third-party organisation to develop the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook ('the Playbook') to help health delivery organizations ('HDOs') prepare for and respond to cybersecurity incidents that involved medical devices. This effort was followed the widespread ransomware attacks affecting HDOs worldwide in 2017, such as WannaCry and Petya/NotPetya.

The Playbook was released in October 2018 by MITRE Corp. The primary audience of the Playbook includes healthcare delivery organisations, clinicians, healthcare technology management professionals, risk managers, facilities staff and information technology personnel involved with emergency response and preparedness. The Playbook provides HDOs with a customisable framework to use as part of their emergency response plans in order to help limit disruptions of continuity of clinical care, as well as divert potential harm to patients.

The Playbook focuses on regional medical device cybersecurity incident preparedness and response, and provides guidance for all phases of medical device incident response, including preparedness, detection and analysis, containment, eradication, recovery, and post-activity analysis.

New Information Sharing and Analysis Organisations

The FDA has entered into two memoranda of understanding to support the creation of new Information Sharing and Analysis Organisations ('ISAOs'): MedISAO and Sensato-ISAO. ISAOs are groups of experts that gather, analyse and disseminate important information about cyber threats. The goal of these ISAOs is to provide manufacturers with the opportunity to share information about potential vulnerabilities and emerging threats with the FDA and to help manufacturers protect patients by addressing issues earlier.

The FDA encourages participation in ISAOs, and considers such participation a critical component of a medical device manufacturer's comprehensive and proactive approach to managing postmarket cybersecurity threats and vulnerabilities. Per the FDA's Postmarket Management of Cybersecurity in Medical Devices guidance ('the Postmarket Guidance'), active participation in an ISAO is one factor in support of a manufacturer avoiding a reportable recall when making changes to address potential vulnerabilities. Given that cybersecurity is a risk that pertains to a number of stakeholders across the healthcare system, open communication regarding the risks and mitigations are critical. Therefore, the FDA has made a concerted effort to provide and facilitate open channels of communication.

The Postmarket Guidance

Although older than a year, the Postmarket Guidance rounds out the efforts described above. It emphasises that manufacturers should monitor, identify, and address cybersecurity vulnerabilities as part of their post market management of medical devices, and establishes a risk-based framework to assess medical device changes and associated cybersecurity vulnerabilities that may surface as part of such changes. The FDA recommends that manufacturers implement a robust postmarket cybersecurity programme that includes, but is not limited to:

- monitoring cybersecurity information sources for the identification and detection of cybersecurity vulnerabilities and risk;
- maintaining robust software lifecycle processes, which include monitoring third party software components for new vulnerabilities, and designing verification and validation for software updates and patches that are used to remediate vulnerabilities;
- understanding, assessing and detecting the presence of vulnerabilities; and

- establishing and communicating the presence and impact of vulnerabilities.

The FDA further emphasises that manufacturers should use a cybersecurity risk management process that allows for the risk to be evaluated and controlled, as well as provide for the monitoring of the effectiveness of the controls. The FDA recommends that the focus should be on assessing the risk of patient harm by considering:

- the exploitability of the cybersecurity vulnerability; and
- the severity of patient harm if the vulnerability were to be exploited.

Given that cybersecurity risks to medical devices are continuously evolving, it is not possible to completely mitigate risks through premarket controls only. Therefore, the FDA's release of the Postmarket Guidance provides stakeholders with information on how to deal with cybersecurity breaches once a product is already on the market.

Conclusion

The momentum of the FDA's efforts in developing a strong cybersecurity platform is only expected to continue in 2019. In August 2019, the FDA plans to participate in DefCon's We 'HEART' Hackers Challenge (a white hat hacker event). In his opening remarks during a 29 January 2019 workshop, the FDA Commissioner, Scott Gottlieb, encouraged manufacturers to volunteer to take the challenge and participate.

The sheer volume of initiatives and communications relating to cybersecurity reflects the FDA's commitment to addressing this growing area of concern for medical devices. As it continues to become more knowledgeable about the risks pertaining to cyber-security, we can expect to see additional initiatives launched to help all stakeholders identify and mitigate these risks.

Yarmela Pavlovic Partner
yarmela.pavlovic@hoganlovells.com
Shilpa Prem Senior Associate
shilpa.prem@hoganlovells.com
Hogan Lovells, San Francisco and Philadelphia

1. See https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm62....
2. §820.30 of Title 21 of the Code of Federal Regulations.

RELATED CONTENT

LEGAL RESEARCH

Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community Code Relating to Medicinal Products For Human Use

NEWS POST

Indonesia: Kominfo announces regulations introducing crypto asset and AML/CTF measures

NEWS POST

Norway: Datatilsynet submits response on medical quality registers regulations consultation

NEWS POST

Germany: BSI opens cybersecurity survey for companies and institutions

NEWS POST

Greece: HDPA issues review of GDPR investigation activities