Compliance & Risks

USA: Medical Device Cybersecurity

Author: Denise McDermott
Senior Regulatory Compliance Specialist, Compliance & Risks

May 31st, 2022

1. Introduction

Cybersecurity has an important role in today's technology-driven world, especially so, with regard to medical devices. There is a growing need for robust cybersecurity processes in the medical device industry, where health information is frequently exchanged across interconnected devices, and as a result, can be vulnerable to cyber threats leading to data breaches of entire software systems or even whole healthcare facilities.

The medical device industry suffered enormously from healthcare data breaches in recent years, with almost 45 million people impacted in 2021 alone according to cybersecurity firm Critical Insights[1]. In 2017 the global WannaCry ransomware attack[2] infected tens of thousands of computers and medical devices, including MRI machines, and continues to this day to be a problem for some organisations.

Furthermore, the SweynTooth cybersecurity vulnerabilities[3] impacted a number of Bluetooth Low Energy devices and due to the gravity of the threat, the US Food & Drug Administration (FDA) published a safety communication in 2020 to medical device manufacturers highlighting the potential danger of such an attack[4].

The FDA stated in the communication that "Security researchers have identified 12 vulnerabilities, named “SweynTooth,” associated with a wireless communication technology known as Bluetooth Low Energy (BLE). BLE allows two devices to “pair” and exchange information to perform their intended functions while preserving battery life."

As a result of these attacks, medical devices were left inoperative, patient care was shut down, and unfortunately, people suffered as a result of the delay in diagnosis and/or treatment, thus demonstrating the frightening reality that old unsecured devices display enormous vulnerabilities and put lives at risk.

It is therefore critical that medical devices have strong cybersecurity systems in place to ensure the safety and effectiveness of these devices and the safety of the patients involved.

This whitepaper will focus on recent developments in medical device cybersecurity in the USA.

2. The Draft Regulations

The FDA issued cybersecurity guidance on “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" in 2014, and the accompanying guidance “Postmarket Management of Cybersecurity in Medical Devices” in 2016.

However, in recent years the global threat of cyber-attacks has increased dramatically and there is a heightened and urgent need for an adequate and consistent reduction of such risks throughout the entire product lifecycle of a medical device. It was, therefore, necessary to update this guide to place greater emphasis on the secure design of medical devices and to describe the FDA's recommendations for premarket submission information in relation to cybersecurity.

On April 8, 2022, the US Food & Drug Administration (FDA) released a draft guidance entitled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions"[5], which applies to devices that contain software or programmable logic, and software as a medical device (SaMD.)

Once finalised, the detail within this guidance document should complement the FDA's “Postmarket Management of Cybersecurity in Medical Devices”, “Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software” and “Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices”, and will replace “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.”

Furthermore, the guidelines and recommendations in this guidance correspond with the advice from the International Medical Device Regulators Forum (IMDRF) final guidance “Principles and Practices for Medical Device Cybersecurity”, issued in March 2020.

The draft guidance "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions", applies to devices as defined in section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) and lays down recommendations surrounding the information to be submitted for devices under certain premarket submission types to demonstrate safety and effectiveness. The submission types include;

- Premarket Notification (510(k)) submissions;
- De Novo requests;
- Premarket Approval Applications (PMAs) and PMA supplements;
- Product Development Protocols (PDPs);
- Investigational Device Exemption (IDE) submissions; and
- Humanitarian Device Exemption (HDE) submissions.

An important point to note is that this guidance document refers to the term “medical device system” indicating the need to consider medical devices as part of a larger overall system. The FDA states that "For the purposes of this guidance, the term “medical device system” includes the device and systems such as health care facility networks, other devices, and software update servers to which it is connected."[5]

The FDA guidance document focuses on four important principles for cybersecurity in medical devices, these being;

A. Cybersecurity is Part of Device Safety and the Quality System Regulations
B. Designing for Security
C. Transparency
D. Submission Documentation

Firstly, the FDA highlights the importance of cybersecurity within the overall context of the quality system. Quality systems requirements are set out in 21 CFR Part 820, the Quality System Regulation (QSR). The FDA recommends that for premarket submission for devices with cybersecurity risks, documentation outputs related to QSR requirements could be submitted to demonstrate safety and effectiveness.

The FDA also encourages manufacturers to consider using a Secure Product Development Framework (SPDF) as a means of achieving QSR requirements. The guidance states; "An SPDF encompasses all aspects of a product's lifecycle, including development, release, support, and decommission.

Additionally, using SPDF processes during device design may prevent the need to re-engineer the device when connectivity-based features are added after marketing and distribution, or when vulnerabilities resulting in uncontrolled risks are discovered."[5]

With regards to designing for security, the FDA requires manufacturers to implement certain security objectives including, authenticity, authorization, availability, confidentiality and secure and timely updatability and patchability. These security objectives must be integrated into the design of the device and this information must be demonstrated in the premarket submission.

The draft guidance also highlights the importance of transparency in relation to cybersecurity. The draft guidance states that "it is important for device users to have access to information pertaining to the device's cybersecurity controls, potential risks, and other relevant information."[5]

Unless such information is shared, cybersecurity risks could go undetected and compromise the safety of the device and are, therefore, an important consideration for device labelling. The final principle covered in this guidance document concerns submission documentation.

The FDA highlights the need for increased documentation when devices are connected to networks or other devices, as the cybersecurity risks are more significant, and a greater level of design control and documentation is required for premarket submission.

The draft guidance recommends the use of a Secure Product Development Framework (SPDF) to control cybersecurity risks for medical devices.

It provides recommendations for using the SPDF processes and documentation for premarket submissions. The recommendations cover (a) security risk management, (b) security architecture and (c) cybersecurity testing.

Security risk management should form part of a manufacturer's quality system, and the FDA proposes the establishment of a security risk management process, that encompasses design controls, validation of production processes, and corrective and preventive actions to address security risks.

A software bill of materials (SBOM) can help in security risk management and the FDA recommends that premarket submissions include the SBOM documentation outlined in section V, subsection A, 2 on security risk management.

Security architecture, as defined in the draft guidance document is "the system and all end-to-end connections into and/or out of the system"[5]. Therefore, the FDA recommends that the entire system should be taken into account when considering the security architecture of a device.

Appendix 2 of the guidance document contains more information on submission documentation for security architecture flows. With regards to cybersecurity testing, the FDA recommends that testing of security requirements, threat mitigation, vulnerability testing and penetration testing, should be provided in the submission. Importantly, the FDA states that cybersecurity testing should occur throughout the SPDF.

The draft guidance document highlights labelling as an important means of informing users of security information pertaining to devices which may aid in the mitigation of cybersecurity risks and should therefore be taken into consideration when drafting labelling for inclusion in a premarket submission.

The FDA outlines a list of fifteen components which it recommends should be included in device labelling to communicate security information to users. Furthermore, the draft guidance recommends that manufacturers establish vulnerability plans to ensure vulnerabilities can be identified and communicated after release to the market.

Overall, given the increased interconnectivity of medical devices coupled with the concerning evolution of sophisticated cybersecurity threats, it is now clear that a total product lifecycle approach to cybersecurity in medical devices is necessary. It is also important for medical device manufacturers to align closely with the expectations of the FDA with regard to premarket submission documentation.

The FDA is accepting comments on the draft guidance document until 7th July 2022.

The proposed Protecting and Transforming Cyber Healthcare ("PATCH") act[6] was introduced on 15th March 2022 to address device cybersecurity concerns. If enacted, the PATCH Act (HR 7084) would amend the Federal Food, Drug, and Cosmetic Act to ensure that all premarket submissions for cyber devices include information that demonstrates conformance to cybersecurity requirements.

The bill defines the term 'cyber device' as a device that (A) includes software, or (B) is intended to connect to the internet. The bill sets out several minimum cybersecurity requirements that manufacturers must attain including those surrounding monitoring and addressing post-market cybersecurity vulnerabilities, developing processes and procedures for updates and patches to the cyber device throughout its lifecycle, coordinated vulnerability disclosure and ensuring manufacturers establish a software bill of materials (SBOM).

The bill states that "The manufacturer shall furnish to the secretary a software bill of materials, including commercial, open-sourced, and off-the-shelf software components that will be provided to users."[6] The SBOM provides a detailed list of the components used in a software application and can improve a device's cybersecurity since the SBOM helps ensure vulnerabilities are detected during design, and easily identifiable post-market.

Overall, the bill aims to introduce statutory requirements that will oblige medical device manufacturers to address cybersecurity going forward.

3. Conclusion

It is critical that medical device manufacturers pay close attention to developments in the area of cybersecurity and invest in establishing vigorous procedures and processes that will guarantee minimal risk going forward. The surge in connected medical devices means the healthcare industry is more vulnerable than ever to cyber threats and ultimately patient harm.

Globally, there is an increased focus on cybersecurity for medical devices and this trend is likely to continue.

Sources

1. Critical Insights report can be found here: https://cybersecurity.criticalinsight.com/2021_H2_HealthcareDataBreachReport
2. Information on the WannaCry Ransomware attack can be assessed here: https://h-isac.org/wannacry-ransomware-update/
3. SweynTooth Vulnerabilities information can be accessed here: https://www.cisa.gov/uscert/ics/alerts/ics-alert-20-063-01
4. The FDA Safety Communication on the SweynTooth vulnerabilities is available at: https://www.fda.gov/medical-devices/safety-communications/sweyntooth-cybersecurity-vulnerabilities-may-affect-certain-medical-devices-fda-safety-communication
5. The draft guidance on Cybersecurity in Medical Devices: Quality System Consideration and Content of Premarket Submissions is available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
6. The proposed “Patch Act;” Proposed “Protecting and Transforming Cyber Health Care” can be accessed here: https://www.congress.gov/bill/117th-congress/house-bill/7084/text

About The Author

Denise McDermott

Senior Compliance Specialist, Compliance & Risks

Prior to joining Compliance & Risks, Denise worked in the medical device industry for 13 years across a number of areas including regulatory affairs, post-market surveillance, customer complaints, quality, and technical support.

She has experience in several areas including IVDR, CE marking, labelling, legal documentation, customer and quality technical communications and regulatory risk assessments.

Unlocking Market Access

Traditionally, tightly controlled due to the impact they may have on human life, Medical Devices are witnessing a further expansion in regulation with recent developments such as the overhaul of the medical device regime in the EU, a focus on medical device traceability, concerns about cybersecurity and more.

These changes, in general, mean that manufacturers of medical devices need to continuously monitor and assess regulatory requirements to ensure compliance. Market Access Solutions built for the modern compliance team.

Manage all of your product compliance activities in one place on a single, powerful, platform with C2P.

Contact us to speak to one of our team today to learn how you can simplify your compliance process.

About Compliance & Risks

At Compliance & Risks, we help you keep on top of regulatory changes and their impact worldwide. Early warning alerts, impact probability, productivity workflow tools and so much more. We have the right technology, regulatory content and expertise to help you unlock market access, protect revenue and elevate the role of compliance.

We provide the broadest and most comprehensive regulatory content on the market, monitoring 195+ countries, 20 industry sectors, 41+ topics and 70,000+ regulatory sources.

For more information, please visit www.complianceandrisks.com

Important Notice: All information provided by Compliance & Risks Limited and its contributing researchers in this report is provided for strategic and informational purposes only and should not be construed as company-specific legal compliance advice or counsel. Compliance & Risks Limited makes no representation whatsoever about the suitability of the information and services contained herein for resolving any question of law. Compliance & Risks Limited does not provide any legal services.