ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)
'A Bridge Between Laboratory and Reader'

www.ijbpas.com

REGULATORY STRATEGIES FOR CYBERSECURITY IN HEALTH CARE: PROTECTING PATIENTS AND DATA

HOVIYA. S. S AND RAJU KAMARAJ*

Department of Pharmaceutical Regulatory Affairs, SRM College of Pharmacy, SRM Institute of Science and Technology, Kattankulathur-603203, Chengalpattu, Tamil Nadu, India

***Corresponding Author: Dr. Raju Kamaraj: E Mail: kamarajr@srmist.edu.in**

Received 20th May 2023; Revised 28th Aug. 2023; Accepted 8th Nov. 2023; Available online 1st Aug. 2024

https://doi.org/10.31032/IJBPAS/2024/13.8.8260

ABSTRACT

The Rapid digitization of medical technologies and the adoption of interconnected systems have revolutionized the healthcare industry, significantly improving patient care and data management. However, this reliance on technology also exposes the healthcare sector to heightened cybersecurity risks. Protecting patients and sensitive medical data from malicious cyber threats has become an imperative concern for regulators, healthcare providers, and patients. The paper explores the evolving landscape of cyber threats faced by healthcare organizations, including data breaches, ransomware attacks, and the compromise of medical devices. It delves into the roles of various stakeholders, such as government bodies, regulatory agencies, healthcare providers, medical device manufacturers, and cybersecurity professionals, in creating a robust cybersecurity ecosystem. It highlights the need for continuous risk assessments, vulnerability monitoring, and incident response planning to mitigate cybersecurity threats effectively. Additionally, the paper emphasizes the significance of building a cybersecurity culture within the medical industry, promoting awareness and training among healthcare staff and patients to enhance the overall security posture.

Keywords: Cybersecurity, Data Protection, Patient Safety, FDA Regulations, Risk Management, Patient Confidentiality

INTRODUCTION

In Healthcare, software is becoming more significant and prevalent. The threats to public health posed by software when it is integrated into a conventional medical device are generally covered by existing legislation. The current implementation of regulations and controls, however, might not always be able to address the particular risks to public health posed by Software as a Medical Device [SaMD] **[1]** and the promotion of public health by encouraging innovation **[2]**.

Medical devices **[1]** is becoming more interoperable and networked to improve patient care. Although interoperability and connectivity may have numerous benefits, linked devices can pose significant cybersecurity concerns **[3]**. A medical device is defined as "an instrument, apparatus, implement, machine contrivance, implant, in vitro reagent, or other similar or related article, including a component part **[4]** With the increased usage of wireless, Internet- and network-connected devices and the regular electronic sharing of health information pertaining to medical equipment, the necessity for strong cybersecurity to ensure medical device operation and safety has become more crucial **[5]**. There are primarily two ways that cybersecurity risks can hurt a healthcare institution by interrupting the operation of medical devices and the integrity of information **[6]**. The overall objective of this is to safeguard and protect any medical information, also known as protected health information, that can be used to identify an individual **[7]**.

The Centre for Devices and Radiological Health [CDRH] of the Food and Drug Administration [FDA] ensures that patients and healthcare professionals have access to reliable medical equipment. This is achieved by FDA post-market surveillance of medical devices and examination of medical device submissions prior to their release on the market **[3]**. Protecting computer systems, networks, and data from interruption or unauthorized access, use, disclosure, modification, or destruction is known as cyber-security **[8]**. Manufacturers should think about cybersecurity-related design inputs for their products as well as a cybersecurity vulnerability and management strategy as part of the software validation and risk assessment mandated by 21 CFR 820.30[g] leading to more effective risk reduction for patients **[5]**.

HARMFUL THREATS OF CYBERSECURITY FOR HEALTHCARE

Healthcare businesses are struggling with the vulnerabilities and potential uses of patient data against patients and organizations as a result of a big difficulty with cybersecurity **[9]**. The hazards of cybersecurity and accessibility to harmful applications in the data of the IoT system have often increased due to various actions such as threats and intrusions into the IoT data infrastructure **[10]**. These hacks can have catastrophic implications on public health and safety in the case of the healthcare sector. The major harmful threats of Cybersecurity to the health sector are Internal Threats, Breach of data, Ransomware, Lack of documented Cybersecurity, Lack of security awareness **[9]**.

KEY ELEMENTS OF A MANAGEMENT PLAN

When creating a strategy for cybersecurity risk management, there should be a mechanism in place to ensure that the communication and implementation of the upgrade are transparent and that there is a minimum amount of downtime for any affected medical devices. Special attention should also be paid to a medical device's labeling and any potential impact that a particular software update or patch may have on the device's intended functionality or regulatory status **[11]**.

IMPORTANCE OF MEDICAL DEVICE DESIGN

Design flaws may also damage a significant portion of MDs. The two most important stages of an MD's TPLC are design and development because a poorly designed device fails to meet regulatory compliance and its inability to safely perform as intended will compromise conformity with Essential Requirements [ERs]. As a part of the requirement of the Quality Management System [QMS], the first rigorous control of an MD is conducted during the design stage. Potential issues can be detected and solved throughout the design phase **[12]**.

CYBERSECURITY REGULATIONS FOR MEDICAL DEVICE SOFTWARE

In order to maintain the operation and safety of medical devices, the FDA guidelines suggest that manufacturers should create cybersecurity measures to ensure the cybersecurity of medical devices **[13]**. The FDA has released premarket and post-market regulatory advice on medical device cybersecurity in acknowledgment of these hazards, and it is actively collaborating with business and outside experts to address post-market cybersecurity issues **[14]**.

- Guidance for Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf [OTS] Software – 2005
- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff – 2014
- Post-market Management of Cybersecurity in Medical Devices –

Guidance for Industry and Food and Drug Administration Staff – 2016

- Content of Premarket Submissions for Device Software Functions-Guidance for Industry and Food and Drug Administration Staff - 2023

Changes to computer software that address cybersecurity vulnerabilities should be verified, according to FDA guidance from 2005. Additionally, the organization advises creating a single cybersecurity maintenance plan **[15]**. The FDA released a draught advice document in June 2013 that discusses how to manage cybersecurity in medical devices during the premarket stage**[16]**. Manufacturers of medical devices must show adequate cybersecurity management when preparing FDA premarket filings. However, as the FDA has emphasised, the same characteristics that make a medical device vulnerable to cybersecurity risks can enhance healthcare and boost medical professionals' capacity to treat patients **[17]**. The FDA guidance advises that security functions should include, but not be limited restricting access to trusted users only, ensuring trusted content, and developing features to enable detecting, responding to, and recovering from a cybersecurity incident **[18]**.

Implementing a proactive, all-inclusive cybersecurity risk management program is advised by the FDA [2016] on post-market management of cybersecurity in medical devices and include monitoring cybersecurity information sources, robust software lifecycle processes, assessing and detecting the presence and impact of vulnerabilities, communication processes for vulnerability and management strategy, and regular use of threat modeling. Deployment of countermeasures to deal with cybersecurity risk early and before exploitation **[19]**.

The objective of FDA recommendations [2023] is to outline FDA's views regarding the suggested documentation sponsors should provide in premarket submissions for FDA's review of the efficacy and safety of device software features **[20]**.

PRE-MARKET CONSIDERATIONS FOR MEDICAL DEVICE CYBERSECURITY

Information about the medical device's cybersecurity should be included in the FDA premarket submission documents, according to FDA -2014 **[5]**. Risk analysis, mitigating measures, design factors, a strategy for distributing verified software patches and updates, ensure the integrity of the software used in medical device, Product specifications and usage instructions for devices relating to suggested cybersecurity measures **[5]**. Software functions that fulfill the definition of a device under section 201[h] of the Federal Food, Drug, and Cosmetic Act [FD&C Act] must provide documentation for premarket submissions for FDA's examination of the safety and efficacy of device software functions. FDA [2023] **[20]**.

A. Software Description

A summary of key software features and operations should be included, together with any illustrations, flowcharts, or state diagrams required to fully describe the functionality of the product. If the premarket application is for a modified device, mention the previous submission's document number and draw attention to any relevant software updates since the last FDA clearance or approval.

B. Risk Management File

The following paperwork should be included in the risk management file, which should be submitted with the premarket submission. For more details on the creation and use of a risk management file, the FDA advises sponsors to consult an FDA-recognized version of ISO 14971.

[1] Risk Management Plan: To demonstrate the efficacy of the risk management activities and procedures for a specific medical device, the FDA advises sponsors to submit a risk management plan. The FDA intends to assess the risk management plan with particular attention to:

- Individual risk acceptability standards that need risk control [reduction].
- A method to assess the acceptability of the total residual risk for all residual risks following the implementation and verification of all risk control measures.

The sponsor's methodology for identifying acceptable risk should serve as the foundation for the risk tolerance criteria. Before doing an initial risk assessment for the device software under review, the acceptability criteria should be outlined in the risk management plan. The risk management strategy should make it apparent how the sponsor intends to weigh the advantages of the anticipated use of the device against the overall residual risk.

[2] Risk Assessment: All device software should come with a risk assessment that covers risk analysis, risk evaluation, risk control, and a benefit-risk analysis. A risk analysis of the system, which includes the software and its entire hardware environment, should be done for any software that is a component of the system. If this information is included in the documentation for the system risk assessment, it should be mentioned in the software documentation with a reference to the relevant premarket submission section.

[3] Risk Management Report: The following should receive a risk management report:

- Demonstrate how the risk management strategy has been properly carried out.

- Confirm that the right individuals have evaluated the risk management file and that the overall residual risk is acceptable.
- Show that adequate procedures are in place for the gathering and evaluation of pertinent pre- and post-production data.

C. Software Requirements Specification [SRS]

Inputs and outputs, functions that the software will perform, hardware performance, interfaces, user interaction, error definition, and handling, intended operating environment, and safety-related requirements derived from a risk assessment are all typically specified in the SRS, which documents the requirements for the software.

The following advice should be taken into account when creating SRS documentation in order to support a prompt premarket review:

- Format the SRS with labeling and/or grouping of needs [such as by modules or units of a function] to make it well-organized, navigable, and readable.
- Make a note of any pertinent traceability between the material in the SRS and other software documents [such as the SDS, System, and Software Architecture Diagram, etc.] that relate to the criteria mentioned in the SRS.
- If the premarket submission involves a change to an already approved or cleared device, make sure to draw attention to any relevant software requirement variances.
- List the specifications that the sponsor considers to be most important [or those that could have the most influence] on the safety and efficiency of the product.
- If any of the information asked above is contained in another document, please indicate this in the submission with an annotation and a link to the page.

D. System and Software Architecture Diagram

The system and software architecture diagram serves as a roadmap for the device design, making it easier to comprehend:

- The components and layers that make up the system and software; the connections between modules and layers; the data inputs, outputs, and data flow between the layers and modules; and
- How users or outside items interface with the system and software, such as IT infrastructure and peripherals [such as wirelessly connected medical devices].

In order to convey the information in a way that can facilitate a productive premarket review, sponsors should provide the right level of detail in the system and software architecture diagram. Additionally, the relationships between the diagrams creating an effective system and software architecture diagram, the sponsor should keep in mind the following visual, linguistic, and reference considerations.

E. Software Design Specification [SDS]

Both a high-level summary of the design and specific design details may be included in the Software Design Specification [SDS]. The fundamental idea that the construction of SDS should take place as a prospective activity rather than documented retrospectively after the software design has been implemented using ad hoc design approaches is reflected in the usage of minimum ad hoc design decisions. Premarket submission parameters for the device function under review should be documented in sufficient depth to identify any anticipated reliance, interoperability, relationship, or utility.

POST-MARKET CONSIDERATIONS FOR MEDICAL DEVICE CYBERSECURITY

According to FDA-2016, To prevent patient harm, cybersecurity risk management programs should place a strong emphasis on addressing vulnerabilities that could lead to unauthorized access, modification, misuse, or denial of use of information stored on, accessed from, or transferred from a medical device to a third party **[19]**. The following are essential elements of such a program:

- Tracking sources of information on cybersecurity to identify and track risks and vulnerabilities;
- Keeping up strong software lifecycle processes with mechanisms for monitoring third-party software components and design verification and validation for software updates and patches that are used to address vulnerabilities.
- Establishing and communicating mechanisms for the input and processing of vulnerabilities; understanding, assessing, and detecting the presence and effect of a vulnerability.

CYBERSECURITY RISK MANAGEMENT FOR MEDICAL DEVICES

A manufacturer should establish, document, and maintain a continuous process for identifying hazards related to the cybersecurity of a medical device, risk analysis, risk evaluation, risk control, and assimilation of production and post-production information throughout the lifecycle of the medical device in accordance with 21 CFR part 820. The procedure by which manufacturers evaluate risks and decide whether a cybersecurity flaw impacting a medical device is an acceptable or unacceptable risk should be clearly defined **[19]**.

RECOMMENDATIONS FOR PMA PERIODIC REPORTS

Information on cybersecurity vulnerabilities, device modifications, and compensating controls put in place in response to this information should be submitted to FDA in a periodic [annual] report for PMA devices subject to periodic reporting requirements under 21 CFR 814.84 **[19]**.

It is advised to give the following details when implementing changes and compensating controls for the device:

- A summary of the firm's risk assessment findings, indicating whether the risk of patient harm was under control or not;
- A brief outline of the modification[s], together with a comparison to the device's earlier certified model and the justification for the modification
- Unique Device Identification [UDI] should be used, If relevant, a link to an ICS-CERT
- A reference to any other pertinent submissions [e.g., PMA Supplement, 30-Day Notice, 806 reports, etc.], if any, or the scientific and/or regulatory

CONCLUSION

The increasing reliance on interconnected medical devices, electronic health records, and telemedicine platforms has presented unprecedented challenges and opportunities for healthcare organizations. The effective implementation of regulatory strategies is of paramount importance and regular risk assessments, vulnerability testing, and incident response planning should be mandated to ensure proactive identification and mitigation of potential cyber risks. The successful implementation of regulatory strategies will not only protect patients' sensitive information but also in still trust and confidence in healthcare services, encouraging patients to medical attention without fear of data breaches or cyberattacks.

ACKNOWLEDGMENT

I am very grateful to SRM College of Pharmacy, SRM Institution of Science and Technology for providing the necessary support, guidance, and facilities.

CONFLICT OF INTEREST

Authors declare no conflict of interest among themselves.

REFERENCES:

[1] Avinash D, Gudipati M, Nadendla RR. Regulatory approach for the approval of Artificial intelligence/Machine language [AI/ML] Based Software as medical devices [SaMD]. International Journal of Research in Pharmaceutical Sciences and Technology. 2020;2[3]:73-8.

[2] Imdrf. IMDRF/SaMD WG/N10FINAL:2013 Final Document Title: Software as a

Medical Device [SaMD]: Key Definitions [Internet]. 2013 [cited 2023 Jul 26].

[3] Schwartz S, Ross A, Carmody S, Chase P, Coley SC, Connolly J, Petrozzino C, Zuk M. The evolving state of medical device cybersecurity. Biomedical instrumentation & technology. 2018 Mar 1;52[2]:103-11.

[4] Jarow JP, Baxley JH. Medical devices: US medical device regulation. In Urologic Oncology: Seminars and Original Investigations 2015 Mar 1 [Vol. 33, No. 3, pp. 128-132]. Elsevier.

[5] FDA-2014. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff Preface Public Comment. 2014.

[6] Busdicker M, Upendra P. The role of healthcare technology management in facilitating medical device cybersecurity. Biomedical Instrumentation & Technology. 2017 Nov;51[s6]:19-25.

[7] Zaldivar D, Lo'Ai AT, Muheidat F. Investigating the security threats on networked medical devices. In2020 10th annual computing and communication workshop and conference [CCWC] 2020 Jan 6 [pp. 0488-0493].

[8] Thakur K, Qiu M, Gai K, Ali ML. An investigation on cyber security threats and security models. In2015 IEEE 2nd international conference on cyber security and cloud computing 2015 Nov 3 [pp. 307-311].

[9] Javaid M, Haleem A, Singh RP, Suman R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications. 2023 Mar 11:100016.

[10] Ahmed G. Improving IoT privacy, data protection and security concerns. International Journal of Technology, Innovation and Management [IJTIM]. 2021;1[1].

[11] Coronado AJ, Wong TL. Healthcare cybersecurity risk management: Keys to an effective plan. Biomedical instrumentation & technology. 2014 May 1;48[s1]:26-30.

[12] Miclăuş T, Valla V, Koukoura A, Nielsen AA, Dahlerup B, Tsianos GI, Vassiliadis E. Impact of design on medical device safety. Therapeutic Innovation & Regulatory Science. 2020 Jul;54[4]:839-49.

[13] Chakrabarti S, Saha HN, Institute of Electrical and Electronics Engineers. New York Section, Institute of Electrical and Electronics Engineers. Region 1, IEEE-USA, Columbia University, et al. 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile

[14] Stern AD, Gordon WJ, Landman AB, Kramer DB. Cybersecurity features of digital medical devices: an analysis of FDA product summaries. BMJ open. 2019 Jun 1;9[6]:e025374

[15] Lechner NH. An overview of cybersecurity regulations and standards for medical device software. InCentral European Conference on Information and Intelligent Systems 2017 [pp. 237-249]. Faculty of Organization and Informatics Varazdin.

[16] Lechner NH. An Overview of Global Professional Publications Related to Medical Device cybersecurity. In Central European Conference on Information and Intelligent Systems 2020 [pp. 221-232]. Faculty of Organization and Informatics Varazdin.

[17] Webb T, Dayal S. Building the wall: Addressing cybersecurity risks in medical devices in the USA and Australia. Computer Law & Security Review. 2017 Aug 1;33[4]:559-63.

[18] Jagannathan S, Sorini A. A cybersecurity risk analysis methodology for medical devices. In2015 IEEE Symposium on Product Compliance Engineering [ISPCE] 2015 May 18 [pp. 1-6].

[19] FDA-2016. Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff

[20] FDA-2023. Content of Premarket Submissions for Device Software Functions Guidance for Industry and Food and Drug Administration Staff This document supersedes Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 2005