# DATA PRIVACY CONCERNS IN SOFTWARE AS A MEDICAL DEVICE (SAMD)

Mrunal Manekar, National Law University Nagpur[1]

Advait Talatule, National Law University Nagpur[2]

## ABSTRACT

In the past few years, medical technology, especially "Software as a Medical Device **(herein after referred to as SaMD)**", has had a big impact on how healthcare is accessible in India. "Software as a Medical Device" is defined by the International Medical Device Regulators Forum (IMDRF) as medical-purpose software that performs its functions independently of a physical medical device. However, alongside these innovations, there exists concerns regarding data privacy and security. A data breach may expose patient or user data stored on the devices, including confidential information, family history, and sensitive medical history. Healthcare data breaches have been a significant and growing problem for years, with a notable surge in recent months. Data Privacy Regulations related to (SaMD) are stated under the purview of Indian Laws but does not cover the aspect completely hence, it is the need of an hour to bring up robust regulations for proper management of data under Software as a Medical Device. Similarly, in context of medical devices, the handling, collection of patient data raises unique concerns. Compliance to the Medical Device Rules, 2017 and International Standards are essential in ensuring data security and regulatory compliance. Interoperability with EHRs, patient consent ethics, and data ownership further complicate the situation. Wearable devices also come under the ambit of Medical devices that collects user's data, then uploads it to the cloud or stores it in a computer. This makes the data collected by wearable devices more likely to be attacked or breached. Defects in technology can also cause problems, such as data and privacy breaches. Addressing concerns about data privacy in medical devices and software is necessary to protect people's rights and build trust in the healthcare and technology ecosystems. The paper will delve into the aspect of regulatory compliance in relation to safeguarding data security and privacy while using Software as a Medical Device.

**Keywords:** Data security, Privacy, Medical devices, Software, Healthcare.

[1] Student at National Law University Nagpur
[2] Student at National Law University Nagpur

## INTRODUCTION

The emergence of the digital revolution in the healthcare sector signifies a dramatic change in the manner in which healthcare services are provided, administered, and experienced. The field of healthcare is witnessing ongoing developments in various technologies, including telemedicine, artificial Intelligence, Machine Learning and wearable devices being used for glucose monitoring and electrocardiography (ECG). Healthcare regulators worldwide are formulating regulations to facilitate the adaptation of each country to the ongoing transformation. The utilisation of software in the medical Device's has witnessed a notable surge due to the swift progression of technology. SaMD pertains to software products specifically designed for medical purposes, including diagnosis and treatment. Nevertheless, the use of SaMD also presents particular risks, specifically with regards to safeguarding data and ensuring cybersecurity. With the growing digitization of the healthcare sector, the significance of cybersecurity in safeguarding patient data and ensuring the security of medical devices cannot be overemphasized. Cyberattacks can result in significant consequences, such as compromising patient safety, breach of confidential information, and interrupting medical services. The occurrence of a cybersecurity breach in a medical device can result in significant consequences, including the compromise of patient data and the disruption of device functionality, thereby posing a potential threat to patient safety. In order to deal with this problem and safeguard the security of patients, it is important to establish strong cybersecurity standards for medical devices. Emphasising the safety of patient data privacy and security is of utmost importance in developing a secure digital healthcare surroundings. Ensuring the reliability, privacy, and safety of SaMD can enhance patient trust and confidence in the healthcare system. The regulation of data collected by SaMDs requires the attention of regulatory bodies, which must develop comprehensive guidelines to protect patient privacy and ensure data security. This paper aims to Critically understand the concept of SaMD and various risks and cybersecurity issues associated with it, Furthermore, it provides a critical analysis of the existing regulations in India, the European Union, and the United States pertaining to the Medical Health data collected and utilised by SaMD.

## RESEARCH OBJECTIVES

1. To understand the concept of software as a medical device and its evolution in healthcare industry.

2. To study and analyze the Data Privacy Concerns associated with SaMD`s.
3. To examine and evaluate the diverse rules and regulations that safeguard Patient Data in the global context of the SaMD`s.

## RESEARCH QUESTIONS

1. What is the concept of software as a medical device and what led to its emergence?
2. What are the various Data Privacy Concerns associated with the use of SaMD`s?
3. What is the approach taken by India and other countries to protect patient data when it pertains to SaMD ?

## AN OVERVIEW OF SaMD AND ITS EVOLUTION.

Over the past few years, there has been rapid technological advancements in the healthcare sector. This rapid advancement in field of healthcare gave rise to the concept of SaMD. Software as a Medical Device, according to the definition given by the "International Medical Device Regulators Forum (IMDRF)"[3], is "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device". SaMD[4] performs its Medical Function without any need for an actual Hardware device[5], it is connected to virtual networks, traditional medical devices, general-use hardware, and non-medical computing platforms. SaMD uses various technologies to diagnose diseases, monitor daily health reports, and notify patients of severe symptoms. The appealing characteristic of SaMD include its ability of transformation of raw data from medical devices, inputs from users and other sources into medical insights, diagnostic information or even actionable medical recommendations.

SaMD is different from SiMD (Software in a Medical Device) as in SiMD, Medical device software cannot function independently or perform its main function without its hardware component. For instance, the software used to programme and operate an MRI machine would

[3] "Software as a Medical Device (SaMD): Key Definitions." International Medical Device Regulators Forum, https://www.imdrf.org/documents/software-medical-device-samd-key-definitions (last visited March 8, 2024).

[4] Software as a Medical Device.

[5]"Software as a Medical Device (SaMD)." U.S. Food And Drug Administration, www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd (last visited March 9, 2024)

be rendered ineffective in the absence of the MRI machine whereas, in the case of SaMD it performs its function independent of any hardware medical device, for instance "A mobile app that monitors a patient's heart rate or glucose levels and makes treatment recommendations to the patient and/or patient's doctor" or even a wearable device that is embedded with Software can be driven by Data Collected by it , *for eg*. a wearable device (SaMD) uses Pulse-oximeter to determine the oxygen level into the blood, various fitness bands, smart watches can even detect if there is a need to visit a doctor. SaMD operates on various platforms such as mobile apps, cloud-based platforms, wearables, and standalone software programmes. It is designed to empower healthcare professionals and patients by providing them with the necessary information[6].

**SaMD includes devices such as software's which analyse:**

Electrocardiogram (ECG)- This kind of software particularly collects users personal data and thereby diagnosing various heart conditions and provides information related to the health of patient`s heart.

Cognitive behaviour (cognitive behavioural therapy) – This therapy collects users personal data which helps people in treatment of various mental conditions by providing users with a pool of exercises and interactive activities which helps them in balancing their mental state.

Diabetes Monitoring- This Software collects user's personal data to monitor glucose level including trade and patterns and inform them with their diet and medication management.

Women's Health- This software collects user's personal data to track their reproductive health, menstrual cycle and provides Personalised insights. All of these software as a medical device collects users personal data and store it with them either in form of cloud storage or input in computers which is although beneficial for user but at the same time this personal data is subjected to certain cybersecurity risks which would be discussed in forthcoming chapters.

Healthcare regulators worldwide are formulating regulations to facilitate the evolution of each country in response to the transformation. In India, Medical device rules 2017 defines SaMD

[6] Bindra, Navraj. "Software as Medical Device in India (SaMD)." NKGABC Blog, (last visited March 12 2024), http://blog.nkgabc.com/software-as-medical-device-in-india/#:~:text=A%20standalone%20medical%20device%2C%20SaMD,a%20medical%20device%20with%20components.

as, “SaMD is a class of software designed to carry out one or more medical functions. It includes software or mobile apps intended to treat, diagnose, cure, mitigate, or prevent disease or other conditions”. In 2020, the To protect user data, quality, and efficacy, Central Drugs Standard Control Organisation issued software as a medical device guidelines. From April 2020, any software or application used to diagnose, prevent, or monitor diseases or disorders, as part of or in combination with a device, or to investigate physical processes will be classified as medical devices and regulated as drugs under the CDSCO Act of 1940.[7]

Further CDSCO considers software a medical device if used for any of the following categories:

1. “Prevention, monitoring, treatment, diagnosis, or alleviation of any disease or disorder

2. Assistance for injuries or disabilities

3. Study evaluation, modification, replacement, or support

4. Life support

5. Disinfection and conception control”.

A list of total 60 Software along with risk classification and intended use was published by CDSCO, SaMD were categorised by risk, intended use, and other factors. This list was the first step towards helping the industry understand software regulations. The CDSCO regulates medical device software import, manufacture, sale, and distribution licences, but not Personal Data.[8], there exists certain cybersecurity threats and legislation related to the issue which will be covered in chapters unfolding.

## DATA PRIVACY CONCERNS ASSOCIATED WITH SAMD`S.

Cybersecurity standards cover a wide range of medical devices (SaMD), including software, firmware, and programmable logic, as well as software used in machine learning algorithms for medical purposes (MLMD). Security measures should include devices that are not

[7] The Drugs And Cosmetics Act, 1940, NO. 23 Acts of Parliament, 1940 (India)

[8] Lenin, Biplab. “Regulating Software as Medical Devices – Navigating Hurdles One Byte at a Time; India Corporate Law.” Cyrilamarchandblogs, (last visited March 19, 2024), corporate.cyrilamarchandblogs.com/2024/03/regulating-software-as-medical-devices-navigating-hurdles-one-byte-at-a-time.

physically/directly connected to networks or other devices but still have software that is vulnerable to cybersecurity attacks. This comprehensive approach aims to ensure strong cybersecurity for all medical/healthcare devices, regardless of connectivity status.

There are various factors such as technical, management, and human causes, which complicates and challenges the protection of data stored in medical devices. Device manuals typically include radio frequency transmission data, while patent databases reveal device operating mechanisms. Outdated software makes data more vulnerable to threats and hackers, while also lacking adequate security measures in medical devices.[9] The utilization of SaMD devices raises concerns regarding privacy due to the collection and sharing of health data. Data breaches have the potential to harm sensitive patient data, including family and medical records. The frequency of healthcare data breaches has experienced a dramatic increase in recent times. CT scanners that detect radiation are susceptible to manipulation, which poses significant concerns to patient safety. System integration is commonly facilitated using web-based services. If there is a requirement for EMR interoperability, it is typically implemented in an insecure manner, involving unsafe authentication and lack of encryption. Data transmitted to EMR systems can be modified. Given the increasing utilization of electronic information systems, ensuring the integrity of health care information is of utmost importance[10]. The incidences of cybersecurity breaches escalate as systems, networks, and devices become more interoperable and integrated. These challenges demonstrate the complexity of cybersecurity risk control and management, widening the health care security gap.[11]

If the medical device is collecting Personally Identifiable Information or any other data that may violate privacy, the transfer of such data may involve huge risk of a data breach. One significant challenge that arises is the issue of medical device network connectivity and support of third party, which is due to the presence of third-party access. Medical device cybersecurity protects devices from unauthorised access, influence, and manipulation, mitigates cybersecurity vulnerabilities, and enables updates, patches, compensating controls, and other upgrades. Our main goal is to assess and develop cybersecurity measures for medical devices to address issues like off-label use, exploitation of unidentified vulnerabilities in the device's

[9] Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, https://www.fda.gov/media/119933/download (last visited March 22).

[10] Patricia AH Williams, Andrew J Woodward, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, NLM, (Last Visited March 19 2024) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/.

[11] Id. At 6.

software or hardware, unauthorised or unsupported user modifications that modify the device to perceived necessitate or choices, and usage in operating environments lacking security measures.[12]

Like other code-enabled systems, medical devices can be vulnerable to design, manufacturing/assembly, implementation, configuration, and vulnerabilities. Some are due to medical device design (plaintext, hard-coded passwords), coding flaws (buffer overflows, command injection), denial-of-service, and malware susceptibility due to missing or improper security patching. The everchanging nature of cybersecurity threats necessitates the implementation of strategic planning and proactive measures in the area of cybersecurity of medical device, taking into account various environmental and usage factors. A cybersecurity incident involving a medical device has the ability to result in physical harm to both patients and users as well as their personal data.

Medical devices like oximeters, hearing aids, and pacemakers can be transformed into spyware and malware, potentially revealing medical data. Experts urge prompt government intervention to address this threat. The caution issued by the researchers is linked to the occurrence of ransomware attacks experienced by one of the most popular hospital chains in India. These attacks resulted in the theft of numerous medical records and significant health data at (AIIMS, Delhi), Safdarjung Hospital. A ransomware attack refers to a type of malware virus in computers that encrypts important documents, making them inaccessible until the attacker or the hacker collects payment in exchange for the encryption key required to unlock them.[13]

Other significant possibilities which can happen and also tells us the need for robust cybersecurity measures are:

***"Possibility of Ransomware Threat to Hospital Systems"***

Ransomware encrypts files, potentially damaging a hospital's EHR system. Backup systems and cybersecurity training are crucial for protecting sensitive information.

[12] John Giantsidis, "Medical Device Security", Asianhhm, (Last Visited March 23,2024) https://www.asianhhm.com/technology-equipment/medical-device-security

[13] Bindu Shajan Perappadan, "Your Medical Device Could Be Spying on You; Industry Demands Protective Laws." The Hindu, (Last Visited March 21 ,2024), www.thehindu.com/news/national/your-medical-device-could-be-spying-on-you-industry-demands-protective-laws/article66710678.ece.

***"Possibility of Unauthorised Access into Telemedicine Systems"***

Telemedicine platforms may be vulnerable to unauthorized monitoring, necessitating immediate software review and updates to ensure security.

***"Potential cloud storage Configuration mistake"***

Cloud-stored patient records may be vulnerable to unauthorised access due to misconfigurations. Cloud security expertise is a crucial requirement for healthcare IT departments.

***"Frequent challenges encountered in mobile applications"***

Healthcare applications storing personal health records and test results may have security vulnerabilities, allowing unauthorised access. App stores may remove apps until security updates are implemented.

***"Potential theft of patient portal identification"***

Malicious individuals can alter patient health data by extracting login credentials.[14]

There is an urgent need as to ensure the development of secured software and prioritising the aspects of cybersecurity of medical devices is crucial for several reasons such as

***"Protecting Patient Safety"***

Cybersecurity breaches and vulnerabilities have the potential to result in unauthorized access to patient data, thereby posing a risk of harm to patients.

***"Protection of sensitive data"***

Medical device collects and stores patients' data and health records. The lack of robust cybersecurity measures and failure to prioritize this data leads to violations of privacy, identity

[14] Weronika Michaluk, "Cybersecurity Best Practices for Software as Medical Device (SaMD)." HTD, (last accessed March 21,2024), htdhealth.com/insights/cybersecurity-software-as-medical-device-samd/#:~:text=Potential%20Insider%20Threat%20Leading%20to,controls%20and%20employee%20access%20permissions.

theft, unauthorize access to medical data and records.

***"Ensuring the Consistency of Care"***

Medical devices have an important role in providing patient care, and any interruption or compromise caused to their data by cybersecurity breaches can have a major consequence. Protection of sensitive data and Ensuring the Consistency of Care. Developing medical device software with strong cybersecurity requires a comprehensive and proactive strategy. Therefore, it is essential to implement Robust cybersecurity measures for medical devices to ensure the dependability, privacy, and protection of SaMD.

## SAFEGUARDING PATIENT DATA RELATED TO SAMD: APPROACH TAKEN BY DIFFERENT COUNTRIES

SaMD offers numerous benefits, including improved diagnostics, personalized treatments, and patient care. However, cybersecurity breaches can compromise patient data and disrupt device functionality, posing a threat to patient safety. To ensure the reliability, privacy, and safety of SaMD, robust cybersecurity measures must be implemented, prioritizing patient data privacy and data security.

In India, the Drugs and Cosmetics Act of 1940[15] governed the use of medical devices as there were no specific medical device related regulations present. The Indian Medical Device Rules , 2017, were introduced by the Central Drug Standard Control Organisation (CDSCO) in order to address this lacuna. These rules serve as the revised regulatory framework for medical devices in India. These regulations cover device classification, registration, manufacturing, imports, packaging, sales, and post-market requirements. There are no direct regulations relating to personal Medical Data or Health data that is being collected by Software as a Medical device, and neither the Medical Rules cover this aspect. However, there are certain regulations and Acts in India where certain references pertaining to the regulation of Data collected by SaMD's are laid down[16]. According to Section 43A I.T Act[17], If a corporate entity responsible for handling sensitive personal data fails to implement and maintain reasonable

[15] The Drugs And Cosmetics Act, 1940, NO. 23 Acts of Parliament, 1940 (India)

[16] Ayushi. "Medical Devices: Compliances and Regulations in India." Life Sciences, Biotechnology & Nanotechnology – India, Mondaq, (last visited March 18th 2024) www.mondaq.com/india/life-sciences-biotechnology--nanotechnology/1143212/medical-devices-compliances-and-regulations-in-india.

[17] The Information Technology Act, 2000 § 43A, No.21, Acts of Parliament, 2000 (India)

security measures, they are liable for any resulting damage due to such negligence. According to Rule 3 of The "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011"[18], medical records and history is included in the ambit of Sensitive Personal Data. Further, the rules also specify that reasonable security practices should be followed (rule 8)[19] and that the body corporate should keep the information secure with them (rule 5)[20].

The Digital Personal Data Protection Act 2023[21] focuses primarily on digital Personal data and does not apply to any non-personal data. The term Personal Data does not distinguish between categories of data such as Sensitive or Critical, it considers any kind of personal data as personal data. Section 2(t)[22] defines personal data as data relating to a person by which he is identifiable. Section 8[23] states that a data fiduciary must protect personal data by implementing reasonable security measures to prevent data breaches. Further, in case of a data breach, the data fiduciary must inform the Data Protection Board and each data principal affected by the breach. The Data Protection Board shall investigate the breach and penalise the data fiduciary. However, the Act does not specify any time limit for reporting the breach.[24]

The newly passed Telecommunication Act of 2023[25] also states certain references pertaining to personal data. Section 2(q)[26] of the Act implies that SaMD will come under the purview of telecommunication equipment, as it uses telecommunication to receive messages related to medical health data. Section 22[27] of the Act states that measures should be taken for the maintenance of cyber security in telecommunication services. However, there is no provision relating to the time frame to notify the authorities about the breach of data, nor are there any provisions laid down mentioning the authority that is responsible for reporting the breach, only the measures that are to be taken to avoid any sort of cyberattack are mentioned.

[18]The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 § Rule 3, Ministry of Electronics and Information Technology, 2011 (India)

[19] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 § Rule 8, Ministry of Electronics and Information Technology, 2011 (India)

[20] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 § Rule 5, Ministry of Electronics and Information Technology, 2011 (India)

[21] The Digital Personal Data Protection Act 2023 No.22, Acts of Parliament, 2023 (India)

[22] The Digital Personal Data Protection Act 2023 § 2(t), No.22, Acts of Parliament, 2023 (India)

[23] The Digital Personal Data Protection Act 2023 § 8, No.22, Acts of Parliament, 2023 (India)

[24] Balasubramanian, Archana. India, New Data Protection Law: Simply Put. Mondaq, (last visited March 21,2024) www.mondaq.com/india/privacy-protection/1417428/indias-new-data-protection-law-simply-put.

[25] The Telecommunication Act of 2023 No.44, Acts of Parliament, 2023 (India)

[26] The Telecommunication Act of 2023 § 2(q) No.44, Acts of Parliament, 2023 (India)

[27] The Telecommunication Act of 2023 § 22 No.44, Acts of Parliament, 2023 (India)

In United states of America, Section 524B[28] of the "Federal Food, Drug, and Cosmetic Act" (FD&C Act) requires medical device manufacturers to take steps to ensure the cybersecurity of their products. This section requires medical device manufacturers to establish cybersecurity threat modelling and risk management, adopt continuous monitoring and risk management plan and report cybersecurity threats to FDA. Manufacturers must create and implement robust post-market monitoring plans to detect and manage medical device risks arising in future, especially cybersecurity risks.[29]

On the other hand, the European Union has the most robust and stringent set of regulations that cover the aspect of SaMD. The EU General Data Protection Regulation[30]'s main objective is to protect personal data of an individual which explicitly includes Data Concerning Health Art. 4(15)[31], meaning any information revealing a person's health status. Art.4(5)[32] states that Data Pseudonymization should take place, which means that processing of data should happen in such a way that it can no longer be identified without the use of additional information. In this way, even if data is breached, it would be very difficult to trace the owner of the health data. Further, the Right to be forgotten is given under GDPR which states that, System must support deletion of personal data if the parties request it. Additionally, Art. 25[33] of GDPR states that data controller should implement data protection measures such as data pseudonymization, data minimization and several data- protection principles. In any Case of Data breach, the data controller must notify the authorities within 72 hours of a data breach. (Art. 33)[34]. Lastly, Art. 35[35] states that there should be a Data protection impact assessment by the data controller before processing of the data to assess the associated risk and implement such measures to address the risks, including safeguards and security measures.

Hence the GDPR is the most prominent and stringent regulation throughout the world that regulates the data collected by SaMD.

[28] Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submission, Guidance for Industry and Food and Drug Administration Staff, https://www.fda.gov/media/119933/download (last visited March 20 2024)

[29] "Cybersecurity." U.S. Food And Drug Administration, www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity. (last visited March 21, 2024)

[30] The General Data Protection Regulations, The European Parliament and Council of European Union (2016), Regulation (EU) 2016/679. gdpr-info.eu. (last visited 25th March 2024)

[31] *Id.* Art. 4(15)

[32] *Id.* Art. 4(5)

[33] *Id.* Art. 25

[34] *Id.* Art. 33

[35] *Id.* Art. 35

In India, though there are certain regulations as discussed above, that cover the aspect of SaMD's but are limited to an extent and are present in bits and pieces thus, there is a need of an hour to bring on robust mechanisms such as the GDPR, such regulations should be amended in the Indian Framework so as to minimize the risk of data breaches in SaMD across India.

## ANALYSIS

Software as a Medical Device is a concept that emerged in the healthcare sector due to technological advancements in telemedicine and AI. The introduction of software as a medical device has been advantageous in certain fields of healthcare, such as ECG analysis, cognitive behavioral therapy, diabetes monitoring, and tracking women's reproductive health. However, there are certain risks associated with its usage, such as cybersecurity threats to the medical data that is stored and data breaches. India has been a target of Medical health data breach that occurred in the AIIMS (Safdarjung) hospital Delhi highlights the vulnerability of data related to health, even though the CDSCO has established guidelines for the classification, registration, manufacturing, and importation of SaMD's however, it does not regulate the aspects of Data breach or privacy related to data stored by SaMD. The DPDA and Telecommunication Act, on the other hand, covers certain facets of medical health data protection, although to a lesser extent as compared to the FDA in the United States and the GDPR in the EU. Hence, it is analyzed that though there are certain regulations present, still India has a long way to go for ensuring the protection of medical health data utilized and stored by SaMD.

## CONCLUSION AND SUGGESTIONS

This paper examines the emerging concept of Software as a Medical Device, focusing on its intended use, storage and utilisation of medical health data and the cybersecurity, privacy threats and vulnerabilities present. Moreover, the paper examines the legislation pertaining to the aspect of SaMD in India and compares it with the European Union and the United States of America. It also explores the necessary advancements India must make in the regulations concerning the privacy of Medical Health Data. The recommendations are based on the fact that data privacy is a crucial aspect of an individual's life, and the regulations do not address certain aspects of a person's medical health data in India. Therefore, specific provisions of the GDPR and the FDA, such as data anonymization, reporting of data breaches within 72 hours, implementation of risk assessment, and post-monitoring plan for continuous assessment of existing software as well as appointment of proper data protection authorities and strict compliance mechanism with stringent penalties should be inculcated in the Indian framework.