Guide to the Software as a Medical Device (SaMD) Regulatory Requirements

By: Asaf Azulay, Rebecca Feldman, September 2020

24 Imber st., Petach Tikva 4951158. | office@li-med.com| www.li-med.com|| |+972-54-8028817

What is Software as a Medical Device (SaMD)?

In the age of rapidly advancing technological innovation, the field of medicine is not left behind. Digital Health and Telemedicine are surging forward with developments in software, Artificial Intelligence and machine learning with the aim of improving patient care.

One of the outcomes of this advancement is the development of Software as a Medical Device (SaMD). The IMDRF (International Medical Device Regulators Forum) is monitoring the rise of SaMD and has issued several guidance documents specifically on the topic of SaMD, upon which the FDA and EU have based their regulatory framework.

SaMD is software which, on its own, is a medical device. This can include software applications intended for treatment, diagnosis, mitigation and prevention of diseases. SaMD may be used in combination with, or interface with, other medical devices, as well as general purpose software.

SaMD includes apps for smartphones, smartwatches and tablets, or computer desktop software that meet the definition of a medical device.

Examples of SaMD include:

- Software that directly controls the hardware of a medical device such as radiotherapy treatment software.
- Software that provides information for immediate decision-making such as blood-glucose monitor software.
- Software that provides support for healthcare professionals such as ECG interpretation software.
- Software for image processing for cancer detection.
- A smartphone app that detects asthma attacks based on changes in voice and breathing.
- A smartwatch app that detects cardiac arrhythmia.
- Software for providing dose recommendations of medications such as insulin, based on patient parameters.

Software as a Medical Device Definition*

Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device.

*IMDRF (International Medical Device Regulators Forum) definition (IMRDF/SaMD WG/N10FINAL:2013)

Is My Software a Medical Device?

First of all, it is important to note that not all software used in the medical profession or a healthcare setting is considered to be a medical device. For example, software for searching a medical database for the retrieval of information is not considered a medical device because it is essentially just a search tool. Other examples include fitness and wellness apps. Stand-alone software that is not part of any hardware that has a medical purpose *and* meets the definition of a medical device is considered SaMD[1].

In the European Union, stand-alone software that does not meet the definition of a medical device but is intended to be an *accessory* of a medical device, will fall under the scope of the European Medical Device Regulation (EU MDR 2017/745) or the European In-Vitro Diagnostic Regulation (IVDR 2017/746).[2]

According to the MDCG 2019 -11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, "software which is intended to process, analyse, create or modify medical information may be qualified as a medical device software if the creation or modification of that information is governed by a medical intended purpose."

Software that is integrated into a medical device is not SaMD, it is considered a component of that medical device and is not regulated separately.

SaMD Regulation

Once it has been determined that a software is a medical device, it will need to be classified according to its intended purpose. If the software is to be marketed in Europe, its classification will follow the rules in Annex VIII of the MDR 2017/745. Rule 11 specifies the classification of medical software.

> In the EU, the software must meet the definition of a medical device or an accessory according to MDR 2017/745 or an IVD according to IVDR 2017/746 in order for these regulations to apply. Otherwise, other EC or national legislations may be applicable.

The IMDRF guidance documents on SaMD provide information on risk-categorization, QMS, Clinical Evaluation as well as responsibilities of the manufacturer.

The FDA and MDCG have published guidance documents which clarify how to apply existing regulations to SaMD and are based on these IMRDF documents. The FDA currently offers a pre-certification program for digital health applications as a pilot program for the development of a future regulatory model for SaMD.

[1] IMRDF/SaMD WG/N10FINAL:2013

[2] MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR

The FDA published a draft guidance on Clinical Decision Support Software that explains how some CDS tools that meet certain criteria are exempt from regulation.[3]

Just like regular medical devices, manufacturers of SaMD will need to establish a Quality Management System in compliance with ISO 13485:2016 (and 21 CFR part 820 in the USA).

As with software incorporated into a medical device, SaMD should be designed and developed in accordance with IEC 62304. This standard describes specific activities for Medical Device Software lifecycle management based on the software's safety class.

Other standards that might apply to SaMD*:

- Usability – IEC 62366
- Health Software - IEC 82304-1
- Risk Management – ISO 14971
- Electrical Safety – IEC 60601
- Information Security Management Systems ISO/IEC 27001

*This list is not exhaustive

SaMD Categorization

The IMRDF[4] defines four risk categories of SaMD based on the levels of impact to the patient or public health. Category IV has the highest level of impact, category I has the lowest.

Determining the risk category of the SaMD depends on the healthcare situation or condition and the significance of the information provided by the SaMD on the healthcare decision. The risk categories appear in the table below:

	Significance of information provided by SaMD to healthcare decision		
Healthcare situation or condition	Treat or diagnose	Drive clinical management	Inform clinical management
Critical	IV	III	II
Serious	III	II	I
Non-serious	II	I	I

A clear SaMD definition statement identifies the intended purpose, states the healthcare situation that the SaMD is intended for and describes the core functionality of the SaMD, enabling the SaMD to be categorized. The SaMD risk category is helpful for determining the classification according to the European regulations.

[3] Clinical Decision Support Software Draft Guidance for Industry and Food and Drug Administration Staff
[4] IMDRF/SaMD WG/N12FINAL:2014

In addition, the IEC 62304 standard for Software Lifecycle Processes of Medical Devices defines three safety classes for medical device software:

- **Class A:** No injury or damage to health is possible
- **Class B:** Injury is possible, but not serious
- **Class C:** Death or injury is possible

This software safety classification determines the safety-related processes that apply to the SaMD.

Similarly, the FDA describes three "Levels of Concern" based on how the operation of the software associated with device function affects the patient or operator.[5]

- **Minor:** injury to patient or operator is unlikely
- **Moderate:** minor injury to the patient or operator, either directly or indirectly.
- **Major:** death or serious injury to patient or operator, either directly or indirectly.

The level of concern determines which documentation must be included in the FDA regulatory submission.

Developing a QMS to Support SaMD

As we mentioned earlier, any manufacturer of a medical device will need to implement a Quality Management System. An effective QMS for SaMD is based on three principles:

- SaMD Leadership and Organizational support
- SaMD lifecycle support processes
- SaMD realization and use processes

There is a strong relationship between these three principles. The leadership and organizational support provide the foundation for the lifecycle support processes, which in turn apply across the realization and use processes.

The diagram below describes the relationship between the principles of the SaMD QMS.

[5] Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

Leadership and Organizational Support

Management is responsible for the lifecycle processes of the SaMD. This includes designating responsibilities and resources for all lifecycle activities to assure the safe and effective performance of the SaMD. The SaMD team should be competent in software engineering and understand the clinical aspects of the SaMD. The infrastructure such as networks, equipment and tools used to support the development, production and maintenance of the SaMD must be provided and maintained.

Lifecycle Support Processes

Efficient product planning is essential to provide direction for the product development lifecycle including definition of phases, milestones and activities, as well as designation of responsibilities and resources. The plan-do-check-act approach is an example of a method for creating a systematic plan for managing products. Planning is dynamic and must be adaptable to changes. For SaMD, it is vital to understand *both* the clinical and software perspective during product planning.

As with any medical device QMS, **document control** and **traceability** are imperative for ensuring productive product design and development. For SaMD in particular, systematic documentation of **configuration** and change management processes is important to enable integration of the SaMD into the clinical environment.

Evaluation of the SaMD and its lifecycle processes involves **measuring and analyzing data** concerning both the software and clinical aspects throughout the lifecycle, with the goal of constantly improving the product. Effective **post-market surveillance** and **vigilance** activities will help identify any nonconformities and determine necessary corrective actions. Any corrective actions taken should be verified and validated before SaMD release.

A SaMD manufacturer that outsources processes, including the use of OTS or SOUP software is responsible for ensuring the quality of the products or services they receive from a supplier or subcontractor.

Risk Management for SaMD

When creating SaMD, it is essential to perform an effective Risk Management process to ensure the safety, effectiveness and performance of the product across the entire lifecycle process in accordance with ISO 14971:2019. SaMD risk management must consider risks relating to patient safety as well as security. The software architecture must integrate risk controls to ensure safety and security.

Realization and Use Processes

One of the first things a SaMD developer should do is define the **requirements** of the product in terms of both the socio-technical environment and clinical needs. These requirements must be captured in the "intended use" of the SaMD that encompasses the healthcare situation or condition and the impact of the information provided by the SaMD to the healthcare decision regarding the patient and public health.

These requirements determine the direction for product design. **Design** activities should lead to the definition of software architecture, components and interfaces of the software which are captured in the **Software Requirements Specifications**. The software architecture must meet user needs and enable other lifecycle processes and activities such as development, verification, validation and maintenance of the SaMD. Safety and security must be integrated into the software architecture and be evaluated at every stage in the product lifecycle.

Development processes turn the requirements, architecture, design, recognized coding practices, and architecture patterns into software items and integrate them into a SaMD product. Development activities should incorporate reviews and follow a defined implementation strategy. The IMRDF document on QMS for SaMD[6] details specific SaMD considerations for design input and the development process.

Verification and Validation (V&V) activities should focus on the criticality and impact to patient safety of the SaMD. Defined V&V activities ensure that all elements from the SaMD design and development have been correctly implemented and the evidence documented. These activities should focus on the interface of the SaMD to the operating system, outsourced components and other elements regarding the computing platform. **Clinical Evaluation** is a core V&V activity.

Deployment activities such as delivery, installation, setup and configuration as well as **servicing** and **maintenance** activities must consider the SaMD lifecycle, realization and use processes and ensure the integrity, safety, effectiveness and performance of the SaMD.

Planning of product realization in the design should include **decommissioning** activities when the SaMD use is terminated. This could entail deactivation and removal of SaMD and data management.

Data Protection and Cybersecurity

Data Protection

In 2018 the **General Data Protection Regulation (GDPR)** came into force in Europe and it applies to all products or applications (not just medical devices) that collect personal data of EU citizens. Similarly, the **Healthcare Insurance Portability and Accountability Act (HIPAA)** in the United States protects personal healthcare data and privacy stored in healthcare and insurance systems. A SaMD that collects personal data must comply with the GDPR and HIPAA. GDPR and HIPAA compliance requires implementation of data security techniques such as pseudonymization, encryption and consent tracking.

[6] IMDRF/SaMD WG/N12

Cybersecurity

Any medical device containing software that is connected to a network is vulnerable to cyber-attacks. Developers of telemedicine and digital health products will need to seriously consider how they will tackle this issue. The FDA and MDCG have issued guidelines on how to implement cybersecurity in medical device software.

The FDA defines two "tiers" of devices according to their cybersecurity risk[7].

- **Tier 1: "Higher Cybersecurity Risk":** a device that can connect to another device, network or the internet ***and*** 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 the criteria for a Tier 1 device are not met.

The aim is for SaMD developers to engineer a system that:

- maintains patient safety and data confidentiality
- maintains the integrity of critical functions
- is resistant to cyber threats such as hacking and viruses

The MDCG guidance document[8] advises how to fulfill the relevant **General Safety and Performance Requirements** of the European MDR and IVDR with regards to cybersecurity. In addition, this guidance document explains how to apply the requirements of other relevant EU regulations such as the Cybersecurity Act, GDPR and NIS Directive.

Cybersecurity should be included in the design and development process of SaMD and appropriate resources designated. The Risk Management Process should evaluate risks related to cybersecurity throughout the lifecycle, and implement appropriate risk controls. Post-Market Surveillance and vigilance processes should be able to recognize cybersecurity issues.

[7] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
[8] MDCG 2019-16 Guidance on Cybersecurity for medical devices

Clinical Evaluation

The purpose of a Clinical Evaluation is to assess and analyze clinical data to verify the safety, performance and effectiveness of a medical device. The IMDRF issued a guideline[9], which has been adopted by the FDA[10], describing the approach to Clinical Evaluation for SaMD. The MDCG issued guidance document[11] for the MDR Clinical Evaluation requirement, which incorporates some of these IMDRF concepts. The Clinical Evaluation process for SaMD is based on three principles:

- Valid Clinical Association
- Analytical/Technical Validation
- Clinical Validation

The Clinical Evaluation process is outlined in the table below:

	Clinical Evaluation		
Step	**Valid Clinical Association**	**Product Performance** V&V Phase of Software Lifecycle	
		Analytical/Technical Validation	**Clinical Validation**
Aim	Is there a valid clinical association between your SaMD output and your SaMD's targeted clinical condition?	Does your SaMD correctly process input data to generate accurate, reliable, and precise output data?	Does use of your SaMD's accurate, reliable, and precise output data achieve your intended purpose in your target population in the context of clinical care?
How	Literature searches, original clinical research, professional society guidelines, secondary data analysis, clinical trials	Accuracy, reliability, precision, repeatability and reproducibility of data	Sensitivity, specificity, odds, ratio, Pre- and post-market

[9] IMDRF/SaMD WG/N41FINAL:2017
[10] Software as a Medical Device (SAMD): Clinical Evaluation - Guidance for Industry and Food and Drug Administration Staff
[11] MDCG 2020-1 Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software

Valid Clinical Association

First, it is important to establish a valid clinical association between the SaMD output and the clinical condition or physiological state. Using a comprehensive literature study, the aim is to determine if the output of the SaMD corresponds to the current state-of-the-art technologies regarding its intended purpose.

Analytical Validation

Second, as part of the performance V&V testing of the SaMD, developers need to determine that the software correctly processes the input data to reliably and accurately deliver the expected output.

Clinical Validation

The third and final step involves additional V&V testing to ensure the use of this output will actually achieve the intended clinical purpose of the SaMD.

Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and **machine learning** have the potential to revolutionize healthcare by improving accessibility, efficiency and effectiveness. However, these new technologies present a host of unique challenges for ensuring safety and performance of an AI medical device. In recent years, standards have been drawn up relating to AI, machine learning and big data and many more are under development.

Such new technologies mean that there is a lack of experience which limits the ability to effectively assess the associated risks. Existing regulatory pathways have not yet been adapted to suit these technologies. However, the FDA has published a discussion paper[12] that describes a framework for a potential approach to regulation of medical device software that incorporates AI and machine learning. Developers of a SaMD which uses AI or machine learning will need to be aware of the changing regulatory landscape.

[12] Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) - Discussion Paper and Request for Feedback

Conclusion

The medical device market has seen an influx of Digital Health software that promises to revolutionize the practice of medicine, opening up new challenges for the regulation of SaMD. The IMRDF guidance documents specifically geared towards SaMD can assist developers navigate QMS, Risk Categorization and Clinical Evaluation. The use of AI and machine learning in medicine have spurred the development of new standards to ensure the safety, effectiveness and performance of SaMD incorporating these technologies. Risk Management of SaMD must consider both risks related to patient safety as well as data protection and cybersecurity. Despite these challenges, SaMD is rapidly paving the way for a brighter, healthier future for all humankind.

Li-Med Can Help

We at Li-Med have been keeping up with the developments in the fields if Digital Health and Telemedicine and are well-versed in all the regulations and guidance documents. Our experts have aided many manufacturers of SaMD to comply with the necessary standards and regulations and swiftly market their device.

Li-Med supports SaMD manufacturers to overcome regulatory hurdles.

We can help with:

- *FDA, CE (MDR) and other regulation*
- *Technical Documentation preparation*
- *Quality Management (ISO 13485 and QSR)*
- *Software Lifecycle management – IEC 62304*
- *Risk Management – ISO 14971*
- *Information Security Management – IEC/ISO 27001*
- *Health Software - IEC 82304-1*
- *HIPAA and GDPR compliance*

Contact us at office@li-med.com for further information.