IMDRF/SaMD WG (PD1)/N23R3

IMDRF International Medical Device Regulators Forum

PROPOSED DOCUMENT

International Medical Device Regulators Forum

Title: Software as a Medical Device (SaMD): Application of Quality Management System

Authoring Group: IMDRF SaMD Working Group

Date: 26 March, 2015

Table of Contents

Preface

The document herein was produced by the International Medical Device Regulators Forum (IMDRF), a voluntary group of medical device regulators from around the world. The document has been subject to consultation throughout its development.

1.0 Introduction

The International Medical Device Regulators Forum (IMDRF) seeks to establish a common and converged understanding for software intended for medical purposes and specifically for a subset of such software that is intended to function as a medical device.

The *IMDRF Software as a Medical Device (SaMD) Working Group (WG)* defines this subset of software as *Software as a Medical Device (SaMD) in the IMDRF SaMD WG N10*[1] document; this document is the foundation for developing a common vocabulary and understanding of SaMD for both manufacturers and regulators.

The SaMD WG has provided a framework to categorize types of SaMD based on impact to public health in the *IMDRF SaMD WG N12* document[2]. This framework establishes a common vocabulary for SaMD, identifies information needed to categorize SaMD, and provides criteria to categorize SaMD based on the combination of the significance of the information provided by the SaMD to the healthcare decision and the healthcare situation or condition where the SaMD is used.

The IMDRF SaMD WG N12 document also highlights the use of quality management as a general consideration towards the safety, effectiveness and performance of SaMD and a key to ensuring the predictability and quality of SaMD.

QMS principles, for many industrial sectors, can be found in the ISO 9000 family of standards. In addition, there are also a wide variety of current industry software development lifecycle methodologies, guidance documents, and standards that address best practices of the many aspects of software engineering quality practices. These principles are the foundation for good practices to maintain and control the quality of products.

In the medical device industrial sector there is a generally accepted principle that following QMS requirements is one of the controls used to avoid and manage unintentional outcomes from the use of medical devices.

In practice, specific QMS requirements for medical devices can either be found in regulatory texts such as Good Manufacturing Practices, in guidance documents from regulators, or in the internationally recognized standard ISO 13485.

Good software engineering is practiced by many software manufacturers to control the quality of their software products. The processes used to accomplish this good engineering practice may readily align with the general principles of QMS requirements.

This document is a companion document to other IMDRF SaMD WG documents, further enabling convergence in vocabulary, approach and a common thinking for regulators and industry.

[1] *IMDRF SaMD WG N10* – "Software as a Medical Device: *Key Definitions*."

[2] *IMDRF SaMD WG N12* - "Software as A Medical Device: *Possible Framework for Risk Categorization and Corresponding Considerations."*

The objective of the document is to provide guidance on the application of existing, standardized and generally accepted QMS practices to SaMD.

This document starts from the perspective of a software development organization (of any size, i.e., could range from a one person enterprise up to a multi-national corporation) that incorporates the activities that are part of good software engineering and quality practices. The document gives an overview of these software quality activities and reinforces medical device quality principles that should be appropriately incorporated for an effective SaMD QMS.

2.0 Scope

The purpose of this document is to:

- Inform the reader, who is assumed to already be following generally accepted software lifecycle processes[3], of SaMD specific practices.
- Create a bridge for software manufacturers who may not be familiar with medical device QMS and how software engineering and software quality practices may apply for SaMD.
- Provide guidance for the application of QMS for the governance of organizations responsible for delivering SaMD products and managing the SaMD lifecycle processes (product planning, risk management, document control and records, configuration management and control, measurement, analysis and improvement of processes and products, and managing outsourced processes and product) and SaMD lifecycle activities (requirements, designing, developing, deploying, maintaining and decommissioning).
- Highlight SaMD lifecycle activities through the lens of patient safety and clinical environment considerations, technology and systems environment considerations that should be addressed to ensure the safety, effectiveness and performance of SaMD.
- Help manufacturers and regulators attain a common understanding and vocabulary for the application of medical device quality management system requirements to SaMD.
- Complement the IMDRF SaMD framework for risk categorization and corresponding considerations [http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf].

This document is intended for the following audience:

- Groups and/or individuals who are or want to become developers of SaMD
- Software development organizations (large or small) that apply good software quality and engineering practices and that may not necessarily be familiar with medical device QMS requirements.
- Organizations (divisions/departments) working within established medical device quality systems that intend to communicate the linkage between medical device quality system practice and SaMD development practices.

Document organization and content:

- Terminology used is intended to be familiar to the software industry and illustrates how typical software-engineering activities (e.g., determining requirements) translate to

[3] These lifecycle processes are intended to include commonly referred lifecycle processes such as software development lifecycle processes (SDLC), software product lifecycle processes (SPLC) and Software System lifecycle processes (SSLC).

equivalent activities in a medical device quality management system (e.g., identifying 'design inputs') used in the management, design, development, implementation, monitoring and support of SaMD.

- Sections are organized based on processes and activities commonly found in software engineering lifecycle approaches as well as the leadership and management of the organization as a whole.
- SaMD lifecycle processes and lifecycle activities include considerations that are necessary to address patient safety and clinical environment as well as the technology and systems environment for SaMD.
- Throughout this document, examples using two fictitious companies – ACME (a large organization) and J&M (a small start-up) — are provided to highlight some of the key points being made.
- ISO13485:2003 is used as the reference material as it is the most widely used QMS standard within the medical device industry.

Field of application:

- The guidance for the application of QMS provided in this document applies to SaMD as defined in the related document, *IMDRF SaMD WG N10 / Software as a Medical Device: Key Definitions* and does not address other types of software.
- This document focuses on SaMD irrespective of technology and/or the platform (e.g., mobile app, cloud, server, etc.).

This document is not intended to:

- Provide guidance on good software engineering practice.
- Rewrite or repeat QMS principles that are articulated in medical device regulations or standards.
- Address software that drives or controls a hardware medical device.

Relationship to regulatory requirements and to technical standards:

- The document does not replace or create new QMS, standards, software engineering practices, or regulations; rather, it highlights common practices and terminology used by successful software organizations.
- This document is not a tutorial on risk management practices for software; rather it highlights risk management principles throughout the software lifecycle processes and activities that are critical to the safety, effectiveness and performance of SaMD.
- The activities highlighted in this document are not meant to replace or conflict with the content and/or development of technical or process standards related to software risk management activities or software development practices.

3.0 References

- IMDRF SaMD WG N10 / Software as a Medical Device: Key Definitions
- IMDRF SaMD WG N12 / Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations
- ISO 13485:2003 – Quality management system – Requirements for regulatory purposes
- ISO 12207:2008 – Systems and software engineering – Software lifecycle processes

4.0 Definitions

This document does not introduce any new definitions but rather relies on the following:

- Definition of SaMD as identified in IMDRF SaMD WG N10 / Software as a Medical Device: Key Definitions and does not address other types of software.
- Terms typically used in standards and regulation as they relate to QMS for medical devices
- Terms and vocabulary used in the software quality practices and software engineering.

5.0 SaMD Quality Management Principles

Medical device QMS principles allow for scaling depending on the type of medical device, risk of the product to patients, size of the organization, technology or automation used to manufacture, and other factors that are determined by the manufacturer to control quality and maintain the safe and effective performance of the medical device.

The manufacturing of SaMD, which is a software only product, is primarily based on the development lifecycle activities often supported by the use of automated software development tools (e.g. build automation, use of a source code management tool, etc.). These automated processes may in some cases replace discrete or deliberate activities (e.g., transfer of design to production) typically found in the manufacturing of hardware products. However, the principles in a QMS that provide structure and support to the lifecycle processes and activities are still applicable and important to control the quality of SaMD.

An effective QMS for SaMD should include all of the following principles:

- A governance structure that provides leadership, accountability and an organization with adequate resources that assures the safety, effectiveness and performance of SaMD (outer circle in figure 1);
- A scalable set of quality processes that apply commonly across SaMD lifecycle processes (middle circle in figure 1); and
- A set of key lifecycle activities that is scalable for the type of SaMD, the size of the organization and takes into account important elements required for assuring the safety, effectiveness and performance of SaMD (innermost circle in figure 1).
- The governance represented by leadership and organizational support is the foundation that supports the management of SaMD lifecycle processes which in-turn supports the SaMD lifecycle activities.

Figure 1: SaMD Quality Management Principles: *Relationship Between Governance, Processes and Activities*

The following references in ISO 13485:2003 are applicable to this section: *4 and 5*

6.0 SaMD Governance: Leadership and Organizational Support

6.1 Leadership and accountability in the organization

Management of the organization is providing the leadership and an overall governance structure for all activities related to the lifecycle activities of SaMD including defining responsibility, authority, and communication of quality objectives for all relevant areas that have an impact on the quality of SaMD. The organization's leadership is also responsible for implementing the QMS, which can include developing a quality policy, quality objectives, and project-specific plans that are customer focused. The governance structure should provide support for creating and establishing appropriate processes that are important for maintaining the quality objectives and policies[4]. In addition the governance should include an overall process for systematically verifying the effectiveness of the established quality management system (periodic QMS internal audit). Management review of the results of the QMS verification is a tool to ensure that the established QMS is suitable, adequate, and effective and makes any necessary adjustments as a result.

Example: In the case of ACME, a product development project is governed at strategic points during a phase-gate process by a cross-functional set of management leaders. As ACME enters the SaMD market, an additional member may need to be added or an existing member may need to take on the additional role of ensuring adherence to patient safety and QMS requirements at all points throughout the product development and deployment lifecycle.

In the case of J&M, each of the principals has been equally responsible and accountable for multiple roles/tasks. As they enter the SaMD market, each will also be responsible for adherence to applicable QMS requirements, with perhaps a designated leader or "enforcer" of applicable QMS requirements.

The following references in ISO 13485:2003 are applicable to this section: *5 and 8.2.2*

6.2 Resource and Infrastructure Management

The purpose of resource management is to provide the appropriate level of resources (including people, tools, environment, etc.), as needed for ensuring the effectiveness of the SaMD lifecycle processes and activities in meeting regulatory and customer requirements.

Example: In ACME, this may be easier to accomplish, as resources and funding for such a management responsibility may exist. However, in the case of J&M, it is something that they will likely research and implement with existing resources.

The following references in ISO 13485:2003 are applicable to this section: *6*

[4] These processes should be tailored specifically towards the needs of the organizations and the level of formal documented processes, objectives and policies should be adjusted appropriately for the type, size and distributed nature of the organization.

6.2.1 People

It is important to ensure that people who are assigned to SaMD projects should be competent to perform their jobs. For SaMD this may include software engineers, engineering managers, testers, etc., who are competent in the technology and software development practices.

Example: In the case of ACME, training and education programs may be well-established and adding specific training for SaMD or hiring trained individuals might be easily accomplished. For J&M, a well-established training program may not exist, however ensuring persons with the right training and educational background to match the SaMD specific tasks required of them are available accomplishes the goal.

The following references in ISO 13485:2003 are applicable to this section: 6.1 and 6.2

6.2.2 Infrastructure and Work Environment

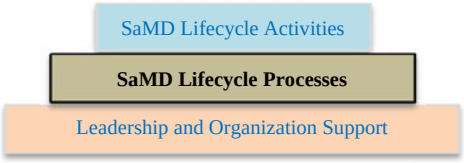
Infrastructure: equipment, information, communication networks, tools, the physical facility, etc., should be made available throughout SaMD lifecycle processes. Such infrastructure is used to support the development, production, and maintenance for SaMD and as such needs to be provided and maintained. For SaMD this may entail identifying and providing the software development and testing environment that simulates the specific technology and configuration and customer needs. These tools should support managing various software configurations during the lifecycle processes, e.g., version management for source code during development, etc.

As the work environment becomes more virtual, the reliability and dependability of the collective infrastructure environment is an important consideration (e.g. dependence on 3rd party networks and equipment).

Example: In the case of ACME, existing computer networks and secure building access might be leveraged directly for SaMD development. However, J&M's development environment (which could have been a single server that was managed virtually and more informally) may need to be separated into multiple environments (e.g., development, QA, staging, demo, production). Doing so would help ensure code integrity, security, reliability, continuity of service to patients and security across these different infrastructure environments in the wake of day-to-day development, upgrades, scheduled and unscheduled maintenance, patches, etc.

The following references in ISO 13485:2003 are applicable to this section: 6.3 and 6.4

7.0 Managing SaMD Lifecycle Processes



An organization's QMS must be built and managed around processes that support the lifecycle activities of SaMD. This section addresses important processes that cut across the SaMD lifecycle activities regardless of the intended use of the SaMD (i.e., significance of the information provided by the SaMD to the healthcare decision and the state of the healthcare situation or condition). There are many available methods to conduct SaMD Lifecycle processes, these processes are typically scaled to address the complexity and size of the SaMD product and project (for e.g. during new product introduction or for an upgrade) that needs to be created.

The sections below: product planning; risk management: a patient safety focused process; document control and records; configuration management and control; measurement, analysis and improvement of processes and product; and managing outsourced processes and product are common processes that are required to be considered throughout the SaMD lifecycle activities regardless of specific approach/method used by the organization. Appropriate implementation of clearly structured and consistently repeatable decision-making processes by SaMD organizations can provide confidence that efforts to minimize patient safety risk and promote patient safety have been considered.

7.1 Product Planning

The objective of planning is to provide a roadmap to be followed during the product development lifecycle. This comes from the quality principle that better results are achieved by following a plan-do-check-act (also known as the PDCA cycle) approach. Product planning includes the definition of phases, activities, responsibilities and resources needed for developing the SaMD. It is important to understand that planning is not static — it needs to be updated when new information is gathered or milestones are reached.

In *IMDRF SaMD WG N12 / Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations* identifies that for SaMD, a thorough understanding of the socio-technical environment (clinical perspective) and the technology and system environment (software perspective) is important in planning as inadequate considerations could lead to incorrect, inaccurate, and/or delayed diagnoses and treatments.[5]

The implementation of SaMD lifecycle activities should adequately be informed and tailored for the type of SaMD as identified in *IMDRF SaMD WG N12*.

Example: The larger Acme Company may have existing planning staff with software based planning tools while the smaller J&M may rely upon other methods. In either case, the plan should be designed to identify tasks to be completed, goals to be achieved, documentation necessary to support the plan and the project, along with appropriate resource and time allocation to achieve the desired results. For both J&M and ACME, this planning phase can employ a model that takes

[5] IMDRF SaMD WG N12 / Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations - Section 9.1 Socio-technical environment considerations and Section 9.2 Technology and system environment considerations.

a deliberate approach to the assignment of resources and reviewed periodically to ensure progress against stated project objectives.

The following references in ISO 13485:2003 are applicable to this section: 5.4, 7.1 and 7.3.1

7.2 Risk Management: A Patient Safety focused process

IMDRF SaMD WG N12 provides a possible framework to categorize types of SaMD based on impact to public health. Using the foundational categorization in *IMDRF SaMD WG N12*, the safety, effectiveness and performance of SaMD, can be assured by appropriate risk management. This risk management process should not be considered singularly in any one process or activity; rather it should be integrated across the entire lifecycle of SaMD.

Just as the general software development industry continuously monitors and manages schedules and budget risks of a software project, a SaMD organization should in addition, and more importantly, monitor and manage risks to patients and users across all lifecycle activities.

For SaMD, lifecycle process and product risk should be informed by the intended purpose, the reasonable foreseeable use, and the understood and defined socio-technical environment of use of the SaMD. Some general considerations associated with SaMD patient safety risk which should be considered throughout the lifecycle activities include the ease with which a SaMD may be updated, duplicated and distributed due to its non-physical nature, and where these updates, made available by the SaMD organization, may be installed by others,

Risk management in the context of this document addresses taking a risk-based approach to patient safety. Specifically, related to QMS, some points that should be considered include:

- The need to identify and act on identified risks
- Actions to address risks and opportunities
- The prevention or reduction of undesired results

For example, it is helpful to chart sources of risk along multiple dimensions, such as:

- User-based risks: Is the SaMD product appropriate for all intended users? For instance, are there risks posed by visual acuity for an elderly user, or for patients with peripheral neuropathy?
- Application-based risks: Should a SaMD application be available on any device, or should it be restricted to certain devices in such a way that it could help to mitigate user risk?
- Device-based risks: Is a device with a smaller screen such as a smartphone adequate for the intended application, can a smaller screen display a large set of information without losing the information or making it cumbersome to the users in a way that could affect patient safety.
- Environment-based risks: Is continuity of use (and therefore, safety) of the SaMD product compromised when there are environmental disruptions (e.g., what happens with use interruptions, background noise, loss of network connectivity during use, etc.)
- Security-based risks: Analysis should include evaluating the security threats to SaMD product software code during manufacturing, maintenance and in-service use. Analysis can also include intrusion detection, penetration testing, vulnerability scanning and data integrity testing to minimize system and patient risks.

Software risk assessment requires a balanced evaluation of both safety and security. Security risks may affect the confidentiality, integrity, and availability of data handled by the SaMD. When considering mitigations to protect device security, the manufacturer should ensure that security risk controls do not take precedence over safety considerations.

Example: For both ACME and J&M, it is useful to create a set of "use-case scenarios", and assess risks in each of the above dimensions by assessing both likelihood of a risk occurring and the associated severity or impact of the risk to the patient. For example, if a patient is entering their weight to track on a smart phone, the likelihood of a "typing error" may be high, but its impact low, as it's merely a weight log. However, if a SaMD product is requiring a patient to enter their weight in order to provide them some form of feedback on medication, or diet, then the impact of the error may be higher, and methods may need to be employed to ensure that the correct value has been entered.

The following references in ISO 13485:2003 are applicable to this section: 7.1

7.3 **Document Control and Records**

Records are used to provide evidence of results achieved or activities performed or not adequately performed as a part of the QMS or SaMD lifecycle processes as well as justifications for QMS activities or SaMD lifecycle processes not performed. Records can be in paper or electronic form.

For SaMD lifecycle processes, document control and records management makes it easier for the users of those documents and records, both within and outside the organization (e.g., outsourced contractors, customers, etc.) to share and collaborate in the many activities related to the SaMD lifecycle process activities, e.g., code development, resolving issues, decommissioning, etc. Document control and records management also serves to help communicate and preserve the rationale for why certain decisions related to SaMD, e.g., related to patient safety or risk management, were made.

Records generated to demonstrate QMS conformity should be appropriately identified, stored, protected, and retained for an established period of time. The following key processes should be integral to managing and maintaining appropriate documentation in the QMS system:

- Reviewing and approving documents before use
- Ensuring current version of applicable documents are available at points of use, (i.e. preventing use of obsolete documents).
- Retaining obsolete documentation for an established period.
- Controlling documents against unauthorized or unintended changes.
- Maintaining and updating documents across all SaMD lifecycle activities.

Example: In the cases of ACME and J&M, it is important to align document complexity with organizational maturity. Documentation does not mean bureaucracy. Rather, it is the basis to drive traceability, repeatability, scalability and reliability in SaMD projects. While ACME may have established documentation processes and techniques that can be used, J&M need not adopt the same processes and techniques that might be necessary for a larger company. Instead, J&M may be able to standardize their existing documentation methods using formally controlled

(reviewed and approved) examples of their current documentation, which may be simpler in nature. Either of these options is acceptable and serves to illustrate the flexibility of applying these concepts and processes.

The following references in ISO 13485:2003 are applicable to this section: 4.2

7.4 Configuration Management and Control

Control of configurable items (including source code, releases, documents, etc.,) is important to maintain the integrity and traceability of the configuration throughout the SaMD lifecycle.

A systematic documentation of the SaMD and its supporting design and development is necessary to identify its constituent parts, to provide a history of changes made to it and to enable recovery/recreation of past versions of the software, i.e., traceability of the SaMD.

For SaMD, configuration is also an important consideration to enable the correct installation and integration of the SaMD into the clinical environment. This information enables users to decide whether or not the SaMD can be used with for example, available hardware, competencies, networks, or whether it is necessary to establish different routines and training or obtain necessary hardware.

In the management of SaMD configuration, software tools are generally used to manage source code, releases, documents, deployment, maintenance, etc. In SaMD, the notion of configuration management and its complexity is amplified by the heterogeneity of the environment in which the SaMD will operate and using the right tools and techniques is important.

Example: For both ACME and J&M, patients can access the SaMD products through multiple devices (e.g., Smartphone, PC, Tablet, etc.) each of which may require specific configurations and optimization of user experiences. This requirement enforces the importance of a robust and documented configuration management process, which might not be well-established at a smaller or newer company such as J&M.

The following references in ISO 13485:2003 are applicable to this section: 4.2.3, 4.2.4, 7.3.7, 7.5.1, and 7.5.3

7.5 Measurement, Analysis and Improvement of Processes and Product

Measurement of quality characteristics of software products and processes is used to manage and improve product realization. An effective measurement process of key factors, often associated with issues related to risk, can help identify the capabilities needed to deliver safe and effective SaMD. Opportunities to monitor, measure and analyze for improvement exist before, during and after a process is completed or the SaMD released and should objectively demonstrate the quality of the SaMD. These processes can include identifying, collecting, analyzing and reporting on critical quality characteristics of products developed.

For SaMD, monitoring, through objective measurement, to demonstrate that processes are being followed does not itself guarantee good software, just as monitoring software quality alone does not guarantee a sufficient process. The effectiveness of the SaMD lifecycle processes and of the

SaMD itself should be evaluated based on predetermined procedures (e.g. leading and lagging safety indicators) to collect and analyze appropriate data. The analyses of this data (including, for example, adverse event reporting, problem reports, bug reports, customer complaints, nonconformity to product requirements, service reports, characteristics and trends of processes and products) are used to evaluate the quality of the SaMD, and the quality of the SaMD lifecycle processes and activities and where/if improvement of these processes and activities can be made.

For SaMD, when a process is not followed correctly, or the SaMD does not meet the quality requirements (i.e., a nonconforming process or product), corrections are required. Nonconforming SaMD should be isolated to prevent unintended use or delivery. The cause of the problem (i.e., SaMD nonconformity) should be analyzed and actions taken to correct or eliminate the problem (i.e., corrective action), and to prevent the same or similar problems occurring in the future. In some cases a potential nonconformity may be identified, and actions such as safeguards and process changes can be taken to prevent nonconformities from occurring (i.e., Preventive Action). Actions taken to address the cause of SaMD nonconformities as well as action taken to eliminate potential SaMD nonconformities should be evaluated for effectiveness.

Lessons learned from the analysis of past projects, including the results from audits of the SaMD lifecycle processes (periodic internal and external) can be used to improve the safety, effectiveness and performance of SaMD lifecycle processes and activities. The manufacturer should also have processes in place for the collection of active and passive post-deployment surveillance information in order to make appropriate decisions relating to future releases.

Example: Preventive actions are often identified during the risk assessment phases of the product realization process. For example, potential risks might be associated with the use of OTS software that exchanges measurement data with the SaMD. Preventive actions to mitigate unacceptable risks from invalid data might be to include fuzz testing of the OTS software during acceptance, and to perform comprehensive error checking of the incoming data during program execution.

The following references in ISO 13485:2003 are applicable to this section: 7.2.3, 8.1, 8.2, 8.3, 8.4, and 8.5

7.6 **Managing Outsourced Processes and Products**

The organization must establish controls that allow it to ensure both, the quality of any outsourced process or product, i.e., any outside software or service supplied to the SaMD organization or integrated into the SaMD (software, contractor, consultant, etc.), and that required process steps within the SaMD lifecycle are being performed. Such controls can include review of deliverables, intermediate result inspection, or audits of the contractor or supplier.

In the case of SaMD, managing outsourced processes and product can include the development of portions of SaMD, the use of 3rd party software or integrating commercial off the shelf (OTS) libraries.

Outsourcing is more effective, when contractors, consultants, or suppliers understand the product and its application domain. For SaMD, where a software module may be outsourced to software contractor(s), it is important to clearly communicate the roles and responsibilities of the software

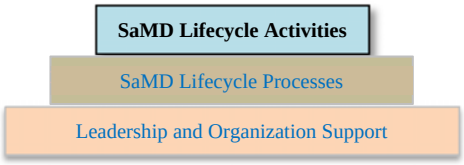
contractor(s) and conditions for the outsourced product through the use of contractual terms to manage or mitigate patient safety risk.

If and when some of the SaMD product is outsourced, i.e., when making use of 3rd party software or integrating OTS software, the SaMD organization is responsible for the safety, effectiveness and performance of the SaMD throughout its lifecycle. For example, when a SaMD incorporates an OTS database (e.g., SQL, etc.), the SaMD organization should understand the capabilities and limitations of the outsourced product throughout the SaMD lifecycle.

Example: ACME and J&M may have historically used open-source code or other OTS code as part of their product development. In the development of SaMD, it is critical for both ACME and J&M, to properly verify and validate the integration of open source code or OTS code. It is also critical to formally evaluate, document, and periodically audit suppliers to ensure compliance with QMS requirements.

The following references in ISO 13485:2003 are applicable to this section: 7.4, 7.4.1, 7.4.2 and 8.5.1.

8.0 SaMD Lifecycle Activities



This section identifies key lifecycle activities that should be identified in the methodologies used in an organization that manufactures SaMD. The following are important perspectives that should be considered for each of the activities in this section.

- SaMD lifecycle processes in Section 7.0 (product planning; risk management: a patient safety focused approach; document control and records; configuration management and control; measurement, analysis and improvement of processes and product; managing outsourced processes and products) should be applied throughout the lifecycle activities.
- This section highlights those activities commonly found in software engineering lifecycle approaches (process, activities, tasks, etc.) that are important for an effective SaMD QMS.
- The activities presented in this section should be included irrespective of methodology used. The presentation of the material does not imply executing the activities in a serial fashion or as discrete phases in the SaMD project (e.g., waterfall process method, etc.); rather these activities should be looked upon as elements to be addressed in any continuous development methodology (e.g., Agile, Extreme, etc.).

The following references in ISO 13485:2003 are applicable to this section: 7

8.1 Requirements

Developing appropriate requirements helps to ensure that SaMD will satisfy the needs across the socio-technical environment including users and patients. These clinical needs should be clearly articulated and the requirements captured in line with the intended use of SaMD as characterized by the "state of the healthcare situation or condition" and the "significance of information provided by SaMD to the healthcare decision" and the resulting impact to public health as identified in *IMDRF SaMD WG N12*.

This is a customer-driven process that requires clear, and often repeated, customer interface to understand the user needs. These user needs are then translated into requirements. Well-documented requirements can then inform the testing activities later in the design cycle. There are other sources of requirements that can include, regulatory or non-customer specified performance requirements.

Patient Safety and Clinical Environment Considerations

- SaMD are used in clinical environments and therefore, in addition to functional requirements, there are requirements that include considerations of user, patient and third party safety. Therefore, some requirements originate from the risk management process that evaluates risks to patients and risk to users and may identify mitigations that become part of requirements.

- Further considerations need to be given to the integrity of data used in the SaMD which may result in specific requirements to ensure that data is secure and to mitigate against the loss or corruption of sensitive data.[6]
- Requirements for SaMD often need to include additional and specific requirements for performing upgrades that consider potential impact to peripheral components of the system as well as appropriate notification and coordination with customers.[7]
- For SaMD, there may be a need to identify and use communication channels that are different from the historical ones (usually involving electronic communication).

Technology and Systems Environment Considerations

- SaMD runs on an underlying platform and operating system, often from a third party. These should be considered as part of the requirements because they can be significant sources of risk.
- Requirements may also need to define non-software aspects of a system.
- Requirements should be captured in concert with stakeholders in the process and should not be captured solely by software or system engineers.

Note: Requirements may change as the developer better understands how the SaMD functions in the clinical environment and as a customer uses it. Therefore, it is important to apply good human factors engineering principles to the development and testing the software to ensure that the requirements were appropriately translated into design inputs.

Example: Whether you are ACME or J&M, requirements serve the purpose of clearly defining what is to be developed in the SaMD product. Requirements also enable traceability of the test outcomes to each requirement. That being said, there are different acceptable ways to capture requirements. In the case of ACME, it is more likely that the existing process and documentation would suffice, and that requirements would be captured by a cross-functional product team to ensure a "360-degree" view of requirements for the SaMD features. In the case of J&M, screen shots, sketches and rapid prototypes that clearly communicate product requirements may also be acceptable. These may also be sufficient to meet the testing traceability needs of the SaMD QMS requirements provided the necessary control of these requirement artifacts is established and maintained and a sense of cross functionality is achieved, either through internal resource collaboration or often, through dialog or workshops with prospective customers and users of the envisaged SaMD product.

The following references in ISO 13485:2003 are applicable to this section: 7.2.1, 7.2.2, 4.2 and 7.1d

[6] IMDRF SaMD WG N12 / Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations - Section 9.3 Information security with respect to safety considerations

[7] IMDRF SaMD WG N12 / Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations - Section 8.2 Changes

8.2 Design

The purpose of the SaMD design activity is to define the architecture, components, and interfaces of the software system, based on user requirements and any other performance requirements in line with the intended use of the SaMD and the clinical / technological environment it will operate in. The requirements are analyzed in order to produce a description of the software's internal structure that will serve as the basis for its implementation. When complete, the SaMD design activity will describe the software architecture, i.e., how the software is decomposed and organized into its components, including considerations for safety critical elements, the interfaces between those components (and any external elements) and a detailed description of each component.

One of the key aspects of the design process is to arrive at a clear and concise design solution that is an effective, well described (e.g., captured in software requirements specifications), logical architecture that best meets the user needs and enables other lifecycle activities such as verification, validation, safe deployment and maintenance of the SaMD.

Patient Safety and Clinical Environment Considerations

- Where a SaMD will be used -- in the home, at the hospital bedside, in a physician's office or clinic -- the users, (e.g. patients, providers and anyone else who can interact or use the information from the SaMD) must be considered in the design activities.
- Clinical risk already identified must be an input to the design phase.

Technology and Systems Environment Considerations

- There are aspects of architectural design that may be driven by the safety critical nature of SaMD and by the risk mitigation solutions, which may include segregation of specific functions into particular modules that are isolated from other areas/modules of the software.
- SaMD design should be robust enough to survive unanticipated upgrades of the underlying platform.

Example: It may be helpful, in an organization of any size, to modularly design SaMD software to allow separability (and hence, scalability) of the data, logic and user-interface (UI) layers. This way, as the SaMD product evolves with either new data fields, new logic or new UI enhancements, it's easier to ensure traceability to SaMD requirements and enable adequate regression testing to make sure "nothing is broken" as a result of the additions.
The following references in ISO 13485:2003 are applicable to this section: 7.3, 7.3.2, 7.3.3, 7.3.4 and 7.3.7

8.3 Development

The development activity transforms the requirements, architecture, design (including interface definition), recognized coding practices (secure) and architecture patterns into software items and the integration of those software items into a SaMD. The result is a software item/system/product that satisfies specified requirements, architecture and design. Good development practice incorporates appropriate review processes, (e.g. code review, peer review, creator self-review, etc.) and follows a defined implementation strategy (e.g. build new, acquire new, re-use of existing elements). Use of appropriately qualified automated tools and supporting infrastructure is important for managing configuration and having traceability to other lifecycle activities.

Patient Safety and Clinical Environment Considerations

- The implementation of clinical algorithms adopted in the code must be clear, in order to avoid misuse or unintentional use.
- The implementation of proper access controls and audit trail mechanisms should be balanced with the usability of SaMD as intended.

Technology and Systems Environment Considerations

- Development activity should leverage the inherent nature of SaMD that allows for efficient methods to understand the user's environment and prevent and manage failures.
- Attention to detail is critical in areas of underlying implementation of the algorithm - a simple data overwrite can potentially lead to an adverse patient safety impact. Some examples of these critical areas include: memory usage and allocation, dependency on communication, speed of operation, and prioritization of tasking, display management and user input capability.
- Many SaMD deal with data entry, and the methods through which data is validated and the impact to the downstream data consumer is an important SaMD consideration.
- As SaMD runs on an underlying platform, rigorous and strict adherence to development guidance as set forth by the platform developer should be followed to ensure backward compatibility.

Example: Software development typically employs a "bug severity" scale (e.g., Severity 1= cosmetic error, Severity 2=functional error, Severity 3=failure, etc.). In SaMD, for both ACME and J&M severity should also be based on patient safety risk related to the healthcare situation or condition[8] (e.g., non-serious, serious, or critical). In other words, there may be bugs that do not cause failures, but that can lead to higher patient safety risk; these instances merit the same attention as a failure. This practice is applicable regardless of the scale of the enterprise.

The following references in ISO 13485:2003 are applicable to this section: 7.3, 7.3.2, 7.3.3, 7.3.4 and 7.3.7

[8] IMDRF SaMD WG N12 / Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations - Section 5.2 Healthcare Situation or Condition

8.4 Verification and Validation

The verification and validation (V&V) activities should be targeted towards the safety-critical nature of SaMD. Typically verification (providing assurance that the design and development activity conforms to the requirements) and validation (providing reasonable confidence the software meets its operational requirements) activities ensure that all elements (including user needs) from the SaMD design and development – including any changes made during maintenance/upgrades – have been implemented correctly and that objective evidence of this implementation is recorded. As SaMD runs on an underlying platform, a defined set of verification and validation activities must focus on that interface to the operating system, outsourced components, and other dependencies.

Patient Safety and Clinical Environment Considerations

- These V&V activities should include scenarios that cover the clinical user/use environment (usability, instructions for use, etc.). This can be accomplished, for example, through structured human factors testing on a subset of patients.
- These activities should confirm that software safety elements work properly (i.e., patient safety / clinical use risk elements, etc.). This is sometimes referred to as "user acceptance testing (UAT)."
- Confirmation of acceptable failure behavior ('fail safe') in the clinical environment should be established.
- Consideration of the socio-technical[9], technology, system environment[10] (sometimes referred to as acceptance/installation testing) should be taken.

Technology and Systems Environment Considerations

- The extent of test coverage as driven by the risk profile of the device as determined by the intended use and SaMD definition statement[11] should be defined and exercised.
- Interoperability of components and compatibility to other platforms/devices/interfaces, etc. with which SaMD works should be considered.
- Provide adequate coverage and traceability to the known risk related functions of SaMD.
- Include the coverage of boundary conditions and exceptions (robustness, stress testing data security, integrity and continuity of SaMD availability).
- Employ rigorous impact analysis of changes made to SaMD (i.e., regression testing) to ensure updates do not compromise the safety, effectiveness and performance of SaMD.

Example: For both ACME and J&M, it is useful to construct test cases that allow a team to first test that the product functions as originally envisaged in the requirements. But, in the case of

[9] Socio-technical systems are systems that include technical systems but also operational processes and people who use and interact with the technical system. Socio-technical systems are governed by organizational policies and rules.

[10] IMDRF SaMD WG N12 / Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations - Section 9.1 Socio-Technical Environment Considerations.

[11] IMDRF SaMD WG N12 / Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations - Section 6: SaMD Definition Statement.

SaMD, it's important to additionally follow up with both clinical user acceptance testing – that is, does the product fulfill its clinically-intended and correct function, as well as human factors testing – that is, can a pre-defined set of inputs be given to multiple users and can the same outcomes be obtained to demonstrate that the product is reasonably usable by most patients? In the latter case, it's often useful to video patients performing the tests to "see" where they get stuck, where they get it right, etc.

The following references in ISO 13485:2003 are applicable to this section: 7.3.5, 7.3.6 and 7.4.3

8.5 **Deployment**

Deployment activities include aspects of delivery, installation, setup, and configuration that support a controlled and effective distribution of SaMD to the customer. As part of risk management, any hazards identified to be mitigated through deployment activities should be addressed in these activities. Some aspects of deployment activities may need to be performed every time a SaMD is distributed to the user (for e.g., distributing an upgrade or fix as a result of maintenance activity). In some cases, especially when SaMD is a large system or is part of a large system, the deployment activities may depend on an extensive collaborative effort with the user (which can include training the users) for an effective use of SaMD or the system.

Patient Safety and Clinical Environment Considerations

- Deploying SaMD into a clinical environment can require considerations of peripheral components if it is intended to be part of a clinical IT network. Therefore, the deployment process often requires the cooperation of hospital IT, integration engineers, clinical engineers, hospital risk managers and others who are often not part of a typical deployment of other products. This may result in the need to define this process clearly to the customer, establishing platform and OS requirements as well as responsibility agreements.
- Deployment needs to consider the end user and end user environment(s) of SaMD. This would be particularly true if used in the home. The deployment process needs to be tailored to the user's abilities and background. Appropriate human factors engineering practices can aid in understanding this aspect and would impact the user requirements capture process.
- Where possible deployment activities should make clearly available (through user documentation and training) to the users any limitations with SaMD (for e.g., limitation of the algorithm, provenance of data used, assumptions made, etc.)
- There should be communication of relevant information to enable correct installation and configuration of the SaMD for appropriate integration with clinical workflows. This can include instructions on how to verify the appropriateness of the installation and update to SaMD as well as any changes made to the system environment.

Technology and Systems Environment Considerations

- Deployment should also include the collection of the settings and the environment of each installation for configuration management. This information should be maintained throughout the life of SaMD at each installation.
- Deployment of SaMD when installed on specific platforms should be according to the intended use that was verified and validated.
- Processes should be in place to ensure the appropriate and correct version is delivered to the user.
- The process of deployment may need to consider integrity of the software to ensure that the software can be delivered in a secure and reliable manner. The choice of deployment method may aid in developing this process.
- Proper deployment methods and procedures are required to ensure repeatability of SaMD delivery, installation, setup, configuration, intended operation and maintenance. It is important to ensure that the computing environments and platforms are sufficient to support proper intended use of the SaMD product.
- Methods that confirm that the software is delivered consistently and comprehensively and that it is used in a defined environment are also important. Non-technical measures may have to be implemented as part of the software product package for deployment. Risk management should highlight dependencies of hazardous scenarios or mitigations on external factors resulting from the computing environment and platforms, the use context and the application processes.
  Note: non-technical measures typically are warning/confirmation dialogs, warning displays, usage notes and user training requirements.

Example: For Both ACME and J&M, when a SaMD is deployed on 'the cloud' or a mobile platform, it is critical to ensure integrity of the deployment process with an extended network of stakeholders. For instance, a SaMD application that is designed for use on a smart phone must be supported with proper processes and documentation that include parties such as the app stores (e.g., iTunes, Google-play, private app clouds, etc.) as well as third party hosting service providers, etc. Unlike the deployment of a gaming app, these extended deployment stakeholders should be qualified and integrated per the QMS requirements for outsourcing and third party supplier management.

The following references in ISO 13485:2003 are applicable to this section: 7.2.3, 7.5, 7.5.1.2.1, 7.5.1.2.2 and 7.5.1.2.3[12]

8.6 **Maintenance**

Maintenance includes activities and tasks to modify a previously deployed SaMD. These activities should preserve the integrity of the SaMD without introducing new safety, effectiveness and

[12] For software products, capabilities like performance, security and safety heavily depend on the computing environment and platforms put in place. The use context and the processes used with the software product will generally influence the above capabilities. Though at the time of deployment or runtime the SaMD organization may have little or no technical control over such factors, the SaMD organization's hazards or mitigations analysis should consider the socio, technical aspects of the intended use and the intended/foreseeable use context of the SaMD

performance risks. Maintenance activities can be adaptive, perfective, preventive and corrective activities originating from SaMD lifecycle processes and activities including in-service monitoring, customer feedback, in-house testing or other information, or changes to user requirements or changes in the socio-technical environment. When these activities require a change to a previously deployed SaMD, all SaMD lifecycle processes and SaMD lifecycle activities should be carried out during the implementation of the change.

To effectively manage the maintenance activities and any resulting changes and their impact to SaMD, a risk assessment should be performed to determine if the change(s) affect SaMD categorization and the core functionality of SaMD as outlined in the SaMD definition statement.[13]

Patient Safety and Clinical Environment Considerations

- Within the context of SaMD it is important to understand how systems, software, context of use, usability, data, and documentation might be affected by changes, particularly with regards to safety, effectiveness and performance;
- As highlighted in other SaMD lifecycle processes and SaMD lifecycle activities, people, technology, and infrastructure and new risks resulting from implementation and use activities should be considered.

Technology and Systems Environment Considerations

- The manufacturer should be aware of any risk impact of changes to architecture and code;
- There should be processes to manage risk arising from changes to system, environment, and data;

Example: In SaMD that involves mobile software development, maintenance can include ensuring that the SaMD product continues to operate as intended when operating system updates (such as iOS, Android, Windows Mobile, etc.) are made. In the case of ACME, a maintenance organization may have resources that are dedicated to watch, track and plan for any residual development or testing required as the OS version changes. In the case of J&M, it may be an "all-hands-on-deck" approach that ensures continuity and integrity of the SaMD product as the new OS version is introduced.

The following references in ISO 13485:2003 are applicable to this section: 7.2.3, 7.5, 7.5.1.2.3, 7.5.4, and 8.2.1

8.7 **Decommissioning (Retirement or End-of-Life activity)**

The purpose of decommissioning activities is to terminate maintenance, support and distribution of SaMD in a controlled and a managed fashion. These activities are important to minimize the public health impact as a result of retiring the SaMD. These activities may include, aspects of configuration management that apply to the document, source code or the delivered SaMD and communicating a plan to the user for gracefully terminating maintenance and support of SaMD.

[13] IMDRF SaMD WG N12 / Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations - Section 8.2 Changes

The process signals an end to active support, and may entail deactivation and/or removal of SaMD and its supporting data. The decommissioning of SaMD data is of special importance, since while the product and/or access may terminate, certain legislations may dictate that the data must be appropriately archived, and not destroyed.

Patient Safety and Clinical Environment Considerations

- Provide clarity to users that no bug fixes, updates, patches or technical support will be available once end-of-life (EOL) is signed-off.
- Appropriately safeguard patient data and any other confidential data. This may include removal, migrating patients to a new SaMD or other product, safe archival of user information, etc.

Technology and Systems Environment Considerations

- Inform customers of important EOL milestones, with sufficient lead-time for users to find, evaluate and qualify possible alternatives.
- Archive a user's environment in an agreed-upon state, which may include steps to protect the security and integrity of information and/or systems.
- Officially document, per QMS guidelines, that the SaMD has been decommissioned.

Example: Medical data may be requested years after the product or its use has been decommissioned. For both ACME and J&M, it is necessary to have effective procedures that ensure effective decommissioning, documentation and data archival for SaMD products.

The following references in ISO 13485:2003 are applicable to this section: 4.2 and 7.

Appendix A - ISO 13485:2003 references

IMDRF/SaMD WG/N23 WD1 (Section)	ISO 13485:2003 (Clause)
5.0--SaMD Quality Management Principles	4 Quality Management System 5 Management Responsibility
6.0--SaMD Governance: Leadership And Organizational Support	--
6.1--Leadership And Accountability In The Organization	5 Management Responsibility 5.1 Management Commitment 5.2 Customer Focus 5.3 Quality Policy 5.4 Planning 5.5 Responsibility, Authority and Communication 5.6 Management Review 8.2.2 Internal Audit
6.2--Resource And Infrastructure Management	6 Resource Management
6.2.1--People	6.1 Provision of Resources 6.2 Human Resources
6.2.2--Infrastructure And Work Environment	6.3 Infrastructure 6.4 Work Environment
7.0--Managing SaMD Lifecycle Processes	--
7.1--Product Planning	5.4 Planning 7.1 Planning of Product Realization 7.3.1 Design and Development Planning
7.2--Risk Management: A Patient Safety Focused Process	7.1 Planning of Product Realization
7.3--Document Control And Records	4.2 Documentation Requirements
7.4--Configuration Management And Control	4.2.3 Control of Documents 4.2.4 Control of Records 7.3.7 Control of Design and Development Changes 7.5.1 Control of Production and Service Provisions 7.5.3 Identification and Traceability
7.5--Measurement, Analysis And Improvement Of Processes And Product	7.2.3 Customer Communication 8.1 Measurement, Analysis and Improvement - General 8.2 Monitoring and Measurement 8.3 Control of Nonconforming Product 8.4 Analysis of Data 8.5 Improvement
7.6--Managing Outsourced Processes And Products	7.4 Purchasing 7.4.1 Purchasing Process 7.4.2 Purchasing Information 8.5.1 Improvement

IMDRF/SaMD WG/N23 WD1 (Section)	ISO 13485:2003 (Clause)
8.0--SaMD Lifecycle Activities	7.0 Product Realization
8.1--Requirements	7.2.1 Determination of Requirements Related to the Product 7.2.2 Review of Requirements Related to the Product 4.2 Documentation requirements 7.1d Records Needed to Provide Evidence That the Realization Processes and Resulting Product Meet Requirements
8.2--Design + 8.3--Development	7.3 Design and Development 7.3.2 Design and Development Inputs 7.3.3 Design and development Outputs 7.3.4 Design and Development Review 7.3.7 Control of Design and Development Changes
8.4--Verification And Validation	7.3.5 Design and Development verification 7.3.6 Design and Development validation 7.4.3 Verification of Purchased Product
8.5--Deployment	7.2.3 Customer Communication 7.5 Production and Service Provision 7.5.1.2.1 Cleanliness of Product and Contamination Control (*as it relates to cybersecurity*) 7.5.1.2.2 Installation Activities 7.5.1.2.3 Servicing Activities
8.6--Maintenance	7.2.3 Customer Communication 7.5 Production and Service Provision 7.5.1.2.3 Servicing Activities 7.5.4 Customer Property (*as it relates to intellectual property and confidential health information)* 8.2.1 Feedback
8.7--Decommissioning	4.2 Documentation Requirements 7 Product Realization

875

IMDRF/SaMD WG/N23 WD1 (Section)	ISO 13485:2003 (Clause)
These clauses from ISO 13485:2003 are not applicable for SaMD.	7.5.3.2.2 Particular Requirements for Active Implantable Medical Devices and Implantable Medical Devices 7.5.5 Preservation of product 7.6 Control of Monitoring and Measuring Devices 8.2.4.2 Particular requirements for active implantable medical devices

876