IMDRF International Medical Device Regulators Forum

FINAL 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: 2 October 2015

Toshiyoshi Tominaga, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2015 by the International Medical Device Regulators Forum.

Table of Contents

1.0 INTRODUCTION 4

2.0 SCOPE 5

3.0 REFERENCES 7

4.0 DEFINITIONS 7

5.0 SAMD QUALITY MANAGEMENT PRINCIPLES 8

6.0 SAMD LEADERSHIP AND ORGANIZATIONAL SUPPORT 10

6.1 LEADERSHIP AND ACCOUNTABILITY IN THE ORGANIZATION 10
6.2 RESOURCE AND INFRASTRUCTURE MANAGEMENT 10
6.2.1 PEOPLE 11
6.2.2 INFRASTRUCTURE AND WORK ENVIRONMENT 11

7.0 SAMD LIFECYCLE SUPPORT PROCESSES 12

7.1 PRODUCT PLANNING 12
7.2 RISK MANAGEMENT: A PATIENT SAFETY FOCUSED PROCESS 13
7.3 DOCUMENT AND RECORD CONTROL 15
7.4 CONFIGURATION MANAGEMENT AND CONTROL 15
7.5 MEASUREMENT, ANALYSIS, AND IMPROVEMENT OF PROCESSES AND PRODUCTS 16
7.6 MANAGING OUTSOURCED PROCESSES, ACTIVITIES, AND PRODUCTS 17

8.0 SAMD REALIZATION AND USE PROCESSES 19

8.1 REQUIREMENTS MANAGEMENT 19
8.2 DESIGN 21
8.3 DEVELOPMENT 22
8.4 VERIFICATION AND VALIDATION 23
8.5 DEPLOYMENT 24
8.6 MAINTENANCE 26
8.7 DECOMMISSIONING (RETIREMENT OR END-OF-LIFE ACTIVITY) 27

APPENDIX A: MAPPING MEDICAL DEVICE REGULATIONS TO IMDRF/SAMD WG/N23 29

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.

There are no restrictions on the reproduction, distribution, or use of this document; however, incorporation of this document, in part or in whole, into any other document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

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 Working Group (WG) defines this subset of software as Software as a Medical Device (SaMD) in the *IMDRF/SaMD WG/N10* document *Software as a Medical Device (SaMD): Key Definitions*; this document is the foundation for developing a common vocabulary; it defines SaMD for both manufacturers and regulators.

The SaMD WG has also provided a framework to categorize types of SaMD based on impact to patient and public health in the *IMDRF/SaMD WG/N12* document *Software as A Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations.* This framework establishes a common approach for categorizing SaMD, using criteria based on the combination of the significance of the information provided by the SaMD to the healthcare decision and on 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 as key to ensuring the predictability and quality of SaMD.

Quality Management System (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 organizations of any size, ranging from a one-person enterprise to a multi-national corporation.

In the medical device sector it is generally accepted that following QMS requirements is one of the controls used to minimize and manage unintentional outcomes related to patient safety. QMS requirements for medical devices are defined by regulatory agencies in their regulations and in the international standard ISO 13485—*Medical Devices—Quality Management Systems—Requirements for Regulatory Purposes*.

In the software industry, good software quality and engineering practices are used to control the quality of software products. These practices may readily align with the general principles of medical device QMS requirements when the patient safety perspective is included.

This document highlights elements of good software quality and engineering practices and reinforces medical device quality principles that should be appropriately incorporated for an effective SaMD QMS.

This is a companion document to *IMDRF/SaMD WG/N10* and *N12* documents, further enabling convergence in vocabulary, approach, and a common thinking for regulators and industry.

2.0 Scope

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

- Inform the reader of SaMD specific practices. It assumes the reader is following generally accepted software lifecycle processes[1] and may not be familiar with medical device QMS;
- Provide guidance for the application of QMS for the governance of organizations responsible for delivering SaMD products and managing the SaMD lifecycle support processes (product planning; risk management; document and record control; configuration management and control; measurement, analysis, and improvement of processes and products; and managing outsourced processes, activities and products) and SaMD realization and use processes (requirements management, design, development, verification and validation, deployment, maintenance, and decommissioning);
- Highlight SaMD realization and use processes from the perspective of patient safety and clinical environment considerations as well as 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; and
- Complement the IMDRF SaMD framework for risk categorization and corresponding considerations found in *IMDRF/SaMD WG/N12*.

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; and
- Organizations (divisions/departments) working within established medical device quality systems that intend to communicate the linkage between medical device quality system practice and software 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 equivalent activities in a medical device quality management system (e.g., identifying

[1] 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).

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 on leadership and management processes of the organization as a whole;
- SaMD lifecycle support processes (Section 7) and realization and use processes (Section 8) include considerations that are necessary to address patient safety and clinical environment as well as the technology and systems environment for SaMD;
- Examples using two fictitious companies—Magna (a large organization) and Parva (a small start-up)—are provided throughout in order to highlight some of the key points being made; and
- References ISO13485:2003, a QMS standard currently published 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 *IMDRF/SaMD WG/N10* and does not address other types of software; and
- This document focuses on SaMD irrespective of technology and/or platform (mobile app, cloud, server, etc.).

This document is not intended to:

- Provide guidance on how to undertake good software quality and engineering practices or how to implement QMSs; and
- Rewrite, repeat, or contradict QMS principles that are articulated in medical device regulations or standards.

Relationship to regulatory requirements and to technical standards:

- The document does not replace or create new QMS standards, software quality and engineering practices, or regulations; rather, it highlights certain common practices and terminology used by successful software organizations;
- This document is not intended to replace or conflict with medical device legislation, regulations, or procedures required in individual regulatory jurisdictions;
- 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; and
- 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 but may provide input to these processes and activities.

3.0 References

- IMDRF/SaMD WG/N10 - Software as a Medical Device (SaMD): 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.

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*.
- Terms typically used in standards and regulations as they relate to QMS for medical devices.
- Terms and vocabulary used in software quality and engineering practices.

5.0 SaMD Quality Management Principles

Medical device QMS principles allow for scaling of activities 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 (build automation, use of source code management tools, etc.). These automated activities 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 the following principles:

- An organizational structure that provides leadership, accountability, and governance with adequate resources to assure the safety, effectiveness, and performance of SaMD (outer circle in *Figure 1*);
- A set of SaMD lifecycle support processes that are scalable for the size of the organization and are applied consistently across all realization and use processes (middle circle in *Figure 1*); and
- A set of realization and use processes that are scalable for the type of SaMD[2] and the size of the organization; and that takes into account important elements required for assuring the safety, effectiveness, and performance of SaMD (innermost circle in *Figure 1*).

[2] As identified by IMDRF SaMD WG N12 document

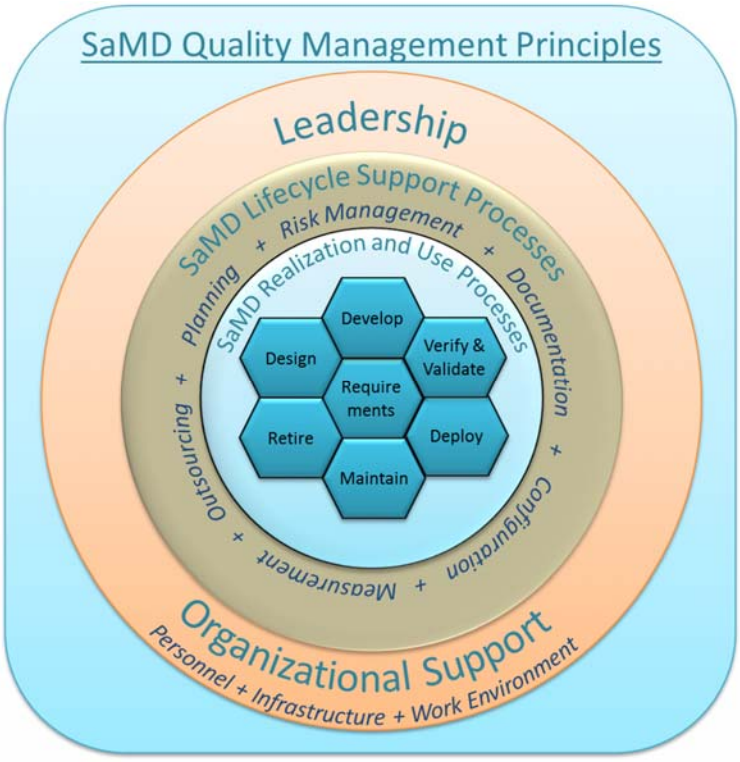


Figure 1: SaMD Quality Management Principles: *Leadership and Organization Support, Processes, and Activities*

The three principles outlined above should not be considered independently as a separate series of processes in an organization. Instead, an effective QMS establishes a distinct relationship (see *Figure 2* below) between the three principles as follows:

- The governing structure of Leadership and Organization Support should provide the foundation for SaMD lifecycle support processes; and
- The SaMD lifecycle support processes should apply across the SaMD realization and use processes.



Figure 2: Relationship between Quality Management Principles

The concepts presented in this section relate to clauses 4 *and* 5 *in ISO 13485:2003.*

6.0 SaMD Leadership and Organizational Support

6.1 Leadership and accountability in the organization

Management of the organization provides the leadership and governance of all activities related to the lifecycle processes of SaMD including defining the strategic direction, responsibility, authority, and communication to assure the safe and effective performance of the 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[3].

In addition, the governance should include activities for systematically verifying the effectiveness of the established quality management system, such as undertaking QMS internal audits. Management review of the results of the QMS audits is a tool to ensure that the established QMS is suitable, adequate, and effective and that any necessary adjustments may be made as a result.

Example: Both Magna and Parva management have responsibilities to ensure that a QMS has been established and that the necessary patient safety considerations have been built in to the QMS and managed when entering the SaMD market. In the case of Magna, the company has an organizational structure that resulted in its Chief Medical Officer being identified as being responsible for these aspects. In the case of Parva, the company has nominated its Software Development Manager to be responsible for including necessary patient safety aspects.

The concepts presented in this section relate to clauses 5 *and* 8.2.2 *in ISO 13485:2003.*

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.

The concepts presented in this section relate to clause 6 *in ISO 13485:2003.*

[3] These processes should be tailored specifically towards the needs of the organizations and the level of 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 in performing their jobs. For SaMD, such a team should have competencies in technology and software engineering including an understanding of the clinical aspects of the use of the software.

Example: Both companies realize the importance of ensuring that there are competent employees to perform their assigned duties. In the case of Magna, there is a broader base of skills amongst the staff with the SaMD skills gap being addressed through an extension of already existing in-house training and education programs. For Parva, the skills gap was bridged by looking to other sources such as temporary recruits and external training programs.

The concepts presented in this section relate to clauses 6.1 *and* 6.2 *in ISO 13485:2003.*

6.2.2 Infrastructure and Work Environment

Infrastructure such as equipment, information, communication networks, tools, and the physical facility, etc., should be made available throughout SaMD lifecycle processes. Such infrastructure is used to support the development, production, and maintenance of SaMD and consequently needs to be provided and maintained.

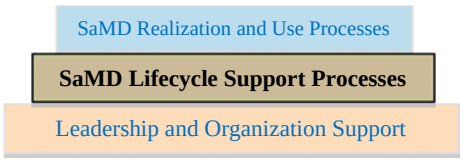
For SaMD, this may entail identifying and providing the software development and test environment that supports the SaMD realization and use processes. This may include providing a test environment that simulates the intended environment of use and tools that support managing various software configurations during the lifecycle processes, e.g., version management for source code during development.

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

Example: Both companies need specific environments for ensuring code and data integrity across these different infrastructure environments. In the case of Magna, existing computer networks and secure building access is leveraged directly for SaMD development. In the case of Parva, the development environment is hosted by a qualified service provider, ensuring the code and data integrity is part of the service agreement between them and the provider.

The concepts presented in this section relate to clauses 6.3 *and* 6.4 *in ISO 13485:2003.*

7.0 SaMD Lifecycle Support Processes



An organization's QMS should be built and managed around processes that support the lifecycle activities of SaMD.

This section addresses important processes that are applicable across the SaMD lifecycle, 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 (e.g., during new product introduction or for an upgrade) that needs to be created.

The elements discussed in this section are common processes and activities that should be considered throughout the SaMD lifecycle regardless of specific software product development approach or 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 can be achieved by following a methodical and rigorous plan for managing projects such as a plan-do-check-act 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.

IMDRF/SaMD WG/N12 identifies that for SaMD, a thorough understanding of the socio-technical[4] 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 processes should adequately be informed and tailored for the type of SaMD as identified in *IMDRF/SaMD WG/N12*.

[4] 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.
[5] *IMDRF SaMD WG N12*: Section 9.1—*Socio-technical environment considerations* and Section 9.2—*Technology and system environment considerations*.

Example: Both companies carry out product planning to decide which operating systems best suited their SaMD application. The larger Magna company has chosen to build its application to work on the top five mobile phone operating systems as the company has the resources to develop on multiple platforms. While the smaller Parva has chosen to develop for the platform that is currently the market leader due to the company's constraints of resources. For both Parva and Magna, this planning phase can allow each company to take deliberate approaches to the assignment of resources.

The concepts presented in this section relate to clauses 5.4, 7.1, *and* 7.3.1 *in ISO 13485:2003.*

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 patient and public health. Using the foundational categorization in *IMDRF/SaMD WG/N12*, the safety, effectiveness, and performance of SaMD can be enhanced by appropriate risk management. This risk management process should be integrated across the entire lifecycle of SaMD.

Organizations that engage in general software development continuously monitor and manage schedules and budget risks of a software project. Similarly, a SaMD organization should also monitor and manage risks to patients and users across all lifecycle processes.

For SaMD, product risk should be informed by the intended purpose; the normal use and reasonably foreseeable misuse; and the understood and defined socio-technical environment of use of the SaMD. Some general considerations associated with SaMD patient safety risk 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, outlines a risk-based approach to patient safety.[6] Specifically, related to QMS, some points that should be considered include:

- Identification of hazards;
- Estimation and evaluation of associated risks;
- Actions to control risks; and
- Methods to monitor effectiveness of the actions implemented to control risks.

[6] ISO 14971:2007 is one commonly used standard that can be used to guide an appropriate medical device risk management process.

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

User-Based

Is the SaMD product appropriate for all intended users? For instance, are there hazards posed by visual acuity for an elderly user, or for patients with peripheral neuropathy? Is the device being used in a clinical or home environment?

Application-Based

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

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

Is continuity of use (and therefore, safety) of the SaMD product compromised when there are environmental disruptions (e.g., interruptions in use, background noise, loss of network connectivity)?

Security-Based

Is analysis being performed that includes evaluating the security threats to SaMD product software code during manufacturing, maintenance and in-service use? Does this analysis also include, for example, intrusion detection, penetration testing, vulnerability scanning, and data integrity testing to minimize system and patient risks?

Software risk management 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: Both Magna and Parva know the importance of carrying out systematic risk management activities throughout their SaMD lifecycles. Magna has a dedicated department whose members ensure that the risk of the product is within acceptable limits, including considerations of patient harm. Parva has chosen to train its SaMD developers in risk-management activities and, with this knowledge, they collectively ensure that the risk of the product is within acceptable limits, including considerations of patient harm. Both of the above approaches ensure that the necessary risk management activities are carried out.

The concepts presented in this section relate to clause 7.1 *in ISO 13485:2003.*

7.3 Document and Record Control

Records are used to provide evidence of results achieved or activities performed as a part of the QMS or SaMD lifecycle processes as well as justifications for any QMS 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 (outsourced contractors, customers, etc.) the organization, to share and collaborate in the many activities related to the SaMD lifecycle processes. Document control and records management also serves to help communicate and preserve the rationale for why certain decisions were made, such as those related to patient safety or risk management.

Records generated to demonstrate QMS conformity should be appropriately identified, stored, protected, and retained for an established period of time. The following activities are examples of ways to manage and maintain appropriate documentation in the QMS system:

- Reviewing and approving documents before use;
- Ensuring current versions of applicable documents are available at points of use to help prevent the use of obsolete documents;
- Retaining obsolete documentation for an established period;
- Controlling documents against unauthorized or unintended changes; and
- Maintaining and updating documents across all SaMD lifecycle processes.

Example: In the cases of Magna and Parva, it is important to manage and control documentation throughout the SaMD lifecycle processes. Documentation does not mean bureaucracy; rather, it is the foundation to drive traceability, repeatability, scalability, and reliability in SaMD projects. Magna uses established documentation processes and techniques that include the use of a commercially available requirements management tool throughout the SaMD lifecycle processes. Parva has re-purposed its source-code control software to enable the company to manage its documentation in a controlled way.

The concepts presented in this section relate to clause 4.2 *in ISO 13485:2003.*

7.4 Configuration Management and Control

Control of configurable items, including source code, releases, documents, software tools, etc., is important in order 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, including a robust and documented configuration and change management process, 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, for example, whether or not the SaMD can be used with available hardware and networks,

whether it is necessary to establish different routines and training, or whether it is necessary to obtain new or reconfigure existing 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; using the right tools and techniques is important.

Example: For Magna and Parva the importance of configuration management is well understood. In both cases the companies' patients can access the SaMD products through multiple devices (e.g., smartphone, PC, and tablet) each of which require specific configurations and optimization of user experiences. The need for multi-device access enforces the importance of a robust and documented configuration management process to ensure the integrity and traceability of the various configurations across product lines.

The concepts presented in this section relate to clauses 4.2.3*,* 4.2.4*,* 7.3.7*,* 7.5.1*, and* 7.5.3 *in ISO 13485:2003.*

7.5 Measurement, Analysis, and Improvement of Processes and Products

Measurement of quality characteristics of software products and processes is used to manage and improve product realization and use. An effective measurement 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 SaMD lifecycle processes, activities and tasks, and are completed with the intent to objectively demonstrate the quality of the SaMD. Post market surveillance including monitoring, measurement and analysis of quality data can include logging and tracking of complaints, clearing technical issues, determining problem causes and actions to address, identify, collect, analyze, and report on critical quality characteristics of products developed. For SaMD, monitoring to demonstrate through objective measurement that processes are being followed does not itself guarantee good software, just as monitoring software quality alone does not guarantee that the objectives for a process are being achieved. Aspects important for the measurement, analysis, and improvement of SaMD processes and products include:

- Evaluation of the SaMD and its lifecycle processes should be based on defined responsibilities and predetermined activities including using leading and lagging safety indicators and collecting and analyzing appropriate quality data. The analysis of this data, such as analysis of customer complaints, problem reports, bug reports, nonconformity to product requirements, service reports, and trends of processes and products should be used to evaluate the quality of the SaMD and the quality of the SaMD lifecycle processes and where/if improvement of these processes can be made. For SaMD, customer complaints may be the major source of the quality data that the organization should analyze.

- Corrections and corrective actions may be required when a process is not correctly followed or the SaMD does not meet its specified requirements (i.e., when a nonconforming process or product exists).
- Nonconforming SaMD should be contained to prevent unintended use or delivery. The detected nonconformity should be analyzed and actions taken to eliminate the detected nonconformity (i.e., correction); and to identify and eliminate the cause(s) of the detected nonconformity (i.e., corrective action) to prevent recurrence of the detected nonconformity 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 actions taken to eliminate potential SaMD nonconformities, should be verified/validated before SaMD release and should be evaluated for effectiveness.
- Lessons learned from the analysis of past projects, including the results from internal or external audits of the SaMD lifecycle processes, can be used to improve the safety, effectiveness, and performance of SaMD. The manufacturer should also have processes in place for the collection of active and passive post market surveillance information in order to make appropriate decisions relating to future releases.
- After the product is in the market, it is important to maintain vigilance for vulnerability to intentional and unintentional security threats as part of post market surveillance.

Example: Customer feedback is an important part of monitoring the performance to improve the product over time. Both Magna and Parva are in the process of developing a new and improved version of their SaMD. Magna has a dedicated department that works independently but in conjunction with sales, marketing, and product development to formally survey its large customer base to gain insights into product performance. In the case of Parva, the company invites some of its early adopters and customers into an office to conduct a round-table discussion to get to the same kind of feedback. Both companies also use embedded analytical tools to gain insights into customer behavior with respect to their use of their respective products. They also routinely review and evaluate customer complaints to identify trends and potential areas for improvement. Based on the review of various sources of data, both Magna and Parva redesigned their SaMD to address common issues identified by customer feedback, complaints, and any new/updated clinical evidence.

The concepts presented in this section relate to clauses 7.2.3, 7.3.7, 7.5.1.1, 8.1, 8.2, 8.3, 8.4, *and* 8.5 *in ISO 13485:2003.*

7.6 Managing Outsourced Processes, Activities, and Products

An effective QMS system takes into account and ensures quality of SaMD when processes, activities, or products are outsourced (i.e., are not completely conducted / made in-house). An organization may choose to outsource different parts of its SaMD process, activities, or product based on its in-house strengths and competencies. Similarly, an organization may procure a commercial-off-the-shelf (COTS) product or another SaMD for integration into its SaMD. In both of these instances, understanding, maintaining control, and managing the effect

of such outsourced processes, activities, or products is important and necessary to deliver safe and effective SaMD.

A SaMD organization may, for example, outsource customer service as a process, or outsource the development activity for a particular module of the SaMD. As with any outsourcing strategy, the following are considerations that are commonly achieved through the use of contractual terms in order to provide confidence in the services and products delivered to manage or mitigate patient safety risk of SaMD:

- Understand the capabilities and competencies of potential outsourcing suppliers;
- Clearly communicate the roles and responsibilities of the outsourcing supplier;
- Extensively define the quality requirements for the outsourced process, activity, or product;
- Clearly establish upfront the criteria for and review of deliverables, frequency of intermediate inspections, and relevant audits of the supplier; and
- Select and qualify the appropriate outsourcing supplier to deliver safe and effective SaMD.

When a SaMD organization plans to procure a COTS product, such as a third-party database for integration in its SaMD, or procure another SaMD to be integrated as a module, the following are examples that may enhance the understanding of the effect of these decisions and help manage the resultant effect on the SaMD:

- Understanding the capabilities and limitations of the COTS product can inform the management of the risks, design choices, and extent of verification and validation needed for the SaMD; and
- Understanding the processes/methods/frequency that the COTS manufacturer employs to update, enhance, or make corrections to its products should be used to inform the selection of the COTS product and the potential effect on the SaMD manufacturer's QMS processes and activities.

Example: Magna and Parva have historically used open-source code or other COTS code as part of product development. In the development of SaMD, it is critical for both Magna and Parva to properly verify and validate the integration of open source code or COTS code. When appropriate, it is also critical to formally evaluate, document, and periodically audit suppliers to ensure compliance with QMS requirements. Both companies are also responsible for monitoring and managing the potential for defects in the COTS, as these defects can contribute to the overall risks of the SaMD and may introduce threats to the larger system within which the SaMD resides. Regardless of the type of code that is used and who is supplying the code, Magna and Parva are ultimately responsible for the safety and performance of the SaMD.

The concepts presented in this section relate to clauses 7.4, 7.4.1, 7.4.2, 7.4.3, *and* 8.5.1 *in ISO 13485:2003.*

8.0 SaMD Realization and Use Processes

This section identifies key lifecycle processes [7] 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 support processes in Section 0 (product planning; risk management: a patient safety focused approach; document and record control; configuration management and control; measurement, analysis and improvement of processes and product; managing outsourced processes and products) should be applied throughout the SaMD realization and use processes.
- 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; rather, these activities should be looked upon as elements to be addressed as part of any development methodology employed.

The concepts presented in this section relate to clause 7 in ISO 13485:2003.

8.1 Requirements Management

Developing appropriate requirements helps to ensure that SaMD will satisfy the needs across the socio-technical environment including those of 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 patient and public health as identified in IMDRF SaMD WG N12.

This is a customer-driven process that requires clear, and often repeated, customer interaction 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.

[7] IEC 62304:2006 is one commonly used software development lifecycle standard that can be used to develop a medical device software lifecycle process.

Patient Safety and Clinical Environment Considerations

- SaMD is used in various clinical and home use environments and, consequently, in addition to functional requirements, there are requirements that include considerations of patient/user safety. Some requirements originate from the risk-management process that evaluates risks to patients and users, and which may identify mitigations that become part of the 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.[8]
- Requirements for SaMD often need to include additional and specific requirements for performing upgrades that consider potential effects on peripheral components of the system as well as appropriate notification and coordination with customers.[9]

Technology and Systems Environment Considerations

- SaMD runs on an underlying platform and operating system, often from a third party, the functionality of which should be considered as part of the requirements, as the platforms and operating systems can be potential sources of harm.
- Requirements may also need to define non-functional aspects of a system such as service or performance related requirements for the hardware platforms that may host the SaMD or means of connecting/networking to the wider environment.
- Requirements should be captured in concert with stakeholders (patients, clinicians, end users, etc.) in the process of use of the SaMD.

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

Example: The definition and maintenance of requirements are important in ensuring that the product meets its intended use. For Magna and Parva, requirements serve the purpose of clearly defining what is to be developed in their respective SaMD products. In the case of Magna, a cross-functional product team leverages existing document templates to capture requirements and an existing document-review process to approve the requirements for use. In the case of Parva, screen shots, sketches, and rapid prototypes are used to refine and capture the product requirements for the SaMD features. In both cases, the requirements are captured in a way that ensures that user, patient, and regulatory requirements are satisfied/met.

The concepts presented in this section relate to clauses 7.2.1, 7.2.2, 7.2.3, 4.2, *and* 7.1d *in ISO 13485:2003.*

[8] *IMDRF SaMD WG N12*: Section 9.3—*Information security with respect to safety considerations*

[9] *IMDRF SaMD WG N12*: Section 8.2—*Changes*

8.2 Design

The purpose of the 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 various clinical and home use environments it is intended to 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 should 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 sufficiently 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 that enables other lifecycle processes and activities such as development, verification, validation, safe deployment, and maintenance of the SaMD.

Building quality into SaMD requires that safety and security should be evaluated within each phase of the product lifecycle and at key milestones. Security threats and their potential effect on patient safety should be considered as possible actors on the system in all SaMD lifecycle activities.
The goal is to engineer a system that: a) maintains patient safety and the confidentiality, availability, and integrity of critical functions and data; b) is resilient against intentional and unintentional threats; and c) is fault-tolerant and recoverable to a safe state in the presence of an attack.

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, clinicians, and others who may interact or use the SaMD) should be considered in the design activities.
- Clinical hazards already identified should be an input in the design phase.

Technology and Systems Environment Considerations

- Architectural design may be driven by the safety critical nature of SaMD and by the risk-mitigation solutions. Risk mitigation solutions may include segregation of specific functions into particular modules that are isolated from other areas/modules of the software.
- SaMD design should have appropriate controls in place to ensure robustness in the event of unanticipated upgrades of the underlying platform.
- SaMD design should include consideration and the taking of appropriate measures when integrating or using software components or infrastructure with limited or uncontrollable knowledge of capabilities and limitations, such as legacy software, undocumented application programing interfaces (API), and wireless network infrastructure.

Such measures should identify the risks that could be introduced to the SaMD product and the extent of implications to the design of the SaMD.

- External resources, sensors, and services used by high-risk aspects of the application should be abstracted such that automated testing can be performed based on consistently simulated values and that operational health considerations can be enforced as a separated concern through mitigated access and mutually understood error conditions.

Example: Magna has a structure within its software department that enables it to distribute the design of different software modules amongst different teams. These teams work in parallel to each other with the interface considerations of the modules being discussed as a specific activity at pre-defined points in the design phase. Parva use uses one multi-disciplined team to develop the design. The company develops its design in an iterative way and considers the internal interfaces as each design effort is complete. Both companies complete their design activity in a controlled and effective manner.

The concepts presented in this section relate to clauses 7.3, 7.3.2, 7.3.3, 7.3.4, 7.3.7 *and* 7.3.1b *in ISO 13485:2003.*

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 activities, (e.g. code review, peer review, creator self-review) and follows a defined implementation strategy (e.g., build new, acquire new, re-use of existing elements). Design changes resulting from the review activity or development activity should be adequately captured and communicated to ensure that other development and QMS activities remain current.

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 should be transparent to the user in order to avoid misuse or unintended 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 event. Some examples of these

critical areas include: memory usage and allocation, dependency on communication, speed of operation, and prioritization of tasks.

- Many SaMD deal with data entry, and the methods through which data is validated and the effect on 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: For both Magna and Parva, coding is central to the delivery of the companies' SaMD product. Magna conducts peer code reviews for SaMD by scheduling periodic peer-review sessions with multiple coders who are not directly involved with the code under review. In the case of Parva, the company does not have a large coding team, and has only one developer who is an expert in his or her chosen operating system. The company uses a technique of "design for code readability", thereby allowing the code review activity to be conducted with a member of the team who is not an expert. Both achieve what is required by good software code review guidelines including the need for independence in the review activity.

The concepts presented in this section relate to clauses 7.3, 7.3.2, 7.3.3, 7.3.4, 7.3.7 *and* 7.3.1b *in ISO 13485:2003.*

8.4 Verification and Validation

The verification and validation (V&V) activities should be targeted towards the criticality and impact to patient safety of the SaMD, as discussed in *IMDRF/SaMD WG/N12*.

Typically, verification (providing assurance that the design and development activity at each development stage conforms to the requirements) and validation (providing reasonable confidence that the software meets its intended use/user needs and operational requirements) activities ensure that all elements 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.

A defined set of V&V activities should focus on the interface of the SaMD to the operating system, outsourced components, and other dependencies related to the computing platform.

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, in part, through structured human factors testing using a subset of patients/clinicians.
- These activities should confirm that software safety elements work properly (i.e., patient safety / clinical use risk elements, etc.). These activities are also commonly included as part of user acceptance testing (UAT).
- Confirmation of acceptable failure behavior in the clinical environment should be established. This may include confirmation of the ability of the software to continue to operate in the specified degraded modes (e.g., fail-safe, fail-secure, or fail-soft).

- Consideration of a variety of user groups to ensure software can be used by persons of different demographics.

Technology and Systems Environment Considerations

- The extent of test coverage should be driven by the risk profile of the device determined by the intended use and SaMD definition statement[10].
- Interoperability of components and compatibility to other platforms/devices/interfaces, etc. with which SaMD works should be considered.
- Adequate coverage and traceability to the known hazard-related functions of SaMD should be provided.
- The coverage of boundary conditions and exceptions (robustness, stress testing, data security, integrity, and continuity of SaMD availability) should be included.
- Companies should 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: In both Magna and Parva, testing coverage and regression testing are important. Magna has a number of test engineers that execute the test plans and regression testing while monitoring coverage. Parva invested in a test automation tool that allows continuous test/build cycle which monitors coverage and regression testing on each checked-in build. Where automation is not possible an independent software developer runs the manual test suite prior to each release. Both companies achieve the appropriate level of test coverage with the necessary levels of independence.

The concepts presented in this section relate to clauses 7.3.5, 7.3.6 *and* 7.4.3 *in ISO 13485:2003.*

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, including any planned risk mitigation for hazards identified throughout the SaMD lifecycle support processes and SaMD realization and use processes.

Some aspects of deployment activities may need to be performed every time a SaMD is distributed to the user (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, such as establishing

[10] *IMDRF SaMD WG N12*: Section 6—*SaMD Definition Statement.*

platform and OS requirements as well as responsibility agreements. The deployment activity should be clearly defined for the customer as the cooperation of hospital IT, integration engineers, clinical engineers, hospital risk managers and others who often may not be part of a typical deployment of other products may often be required.

- Deployment needs to consider the end user and use environment(s) of SaMD. This would be particularly true if used in the home. The deployment activity needs to be tailored to the user's abilities and background. Appropriate human factors engineering practices can aid in understanding this aspect and would affect the user requirements capture activity.
- Where possible, user documentation and user training materials should identify any limitations with SaMD. These may include limitations of the algorithm, provenance of data used, assumptions made, etc., that should be considered during deployment.
- 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 choice of deployment method should consider the integrity of the SaMD to ensure that the software can be delivered in a secure and reliable manner.
- Deployment methods and procedures should ensure repeatability of SaMD delivery, installation, setup, configuration, intended operation, and maintenance.
- 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.
- When deploying an update to SaMD, updating user manual(s), anomaly lists, or providing training may be necessary.

Note: Non-technical measures can include warning/confirmation dialogs, warning displays, usage notes, and user training requirements.

Example: For Both Magna and Parva, when a SaMD is deployed on 'the cloud' or a mobile platform, it is critical to ensure integrity of the deployment activity with an extended network of stakeholders. For instance, a SaMD application that is designed for use on a smart phone should be supported with proper processes and documentation that include parties such as app stores

and private app clouds, as well as third-party hosting service providers, etc. Unlike the deployment of general consumer software, for example, these extended deployment stakeholders should be qualified and integrated per the QMS requirements for outsourcing and third-party supplier management.

The concepts presented in this section relate to clauses 7.2.3, 7.5, 7.5.1.2.1, 7.5.1.2.2, 7.5.1.2.3[11] *and* 7.5.5 *in ISO 13485:2003.*

8.6 Maintenance

Maintenance includes activities and tasks to modify a previously deployed SaMD. Maintenance activities can be adaptive, perfective, preventive, and corrective activities originating from software 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 a previously deployed SaMD requires maintenance, all appropriate SaMD lifecycle support processes, and SaMD realization and use processes should be considered. Maintenance activities should preserve the integrity of the SaMD without introducing new safety, effectiveness, performance, and security hazards.

To effectively manage the maintenance activities and any resulting changes and their effect on 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.[12]

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.
- The SaMD manufacturer should take into account implications and introduction of patient safety risk as a result of changes to architecture and code.
- As highlighted in other SaMD lifecycle processes and SaMD lifecycle activities, people, technology, infrastructure, and new hazards resulting from implementation and use activities should be considered.
- It is important to understand the effect of the change on patient safety and the need for addressing the change in a timely manner when appropriate.

[11] 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

[12] *IMDRF SaMD WG N12* - Section 8.2 Changes

Technology and Systems Environment Considerations

- There should be processes that manage risk arising from changes to system, environment, and data.
- SaMD manufacturers should make it feasible for users to safely implement information security updates.
- Instructions for users related to information security should include how to safely update security software/spyware, operating environment, and other systems and applications, etc.

Example: Magna has a process that controls change of its SaMD through a change-control board. This is a multi-disciplined team that meets at regular intervals to review the change requests and recommend (or reject) them for incorporation in the next version of software. Parva has assigned its project manager to act as a customer representative; as part of this role, she reviews the feedback items received and adds any relevant issue to the backlog of the next release. Both companies prioritize the change requests to ensure that any significant issues are dealt with in a timely manner.

The concepts presented in this section relate to clauses 7.2.3, 7.5, 7.5.1.2.3, 7.5.4, 7.6 *and* 8.2.1 *in ISO 13485:2003.*

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. Although not specifically mentioned in ISO 13485 as a clause, the standard does require planning of product realization in the design which would include decommissioning.

Decommissioning activities are important to minimize the impact to patient and public health safety 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.

This process indicates 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. While the product and/or access may be terminated, there may be country specific requirements for managing the data.

Patient Safety and Clinical Environment Considerations

- Provide clarity to users which services (e.g., bug fixes, updates, patches, technical support, etc.) 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 another 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.

Example: For both Magna and Parva, it is necessary to have procedures that ensure effective decommissioning, documentation, and data archival for SaMD products. Both have a process that asks for a decommissioning plan to be created. This plan takes consideration of the following points to arrive at an effective solution for decommissioning a SaMD:

- *What minimum retention time periods are defined by each territory in which the devices are marketed;*
- *Will any data be migrated onto new/replacement devices/software systems and, if so, will any data conversion be needed and how will this be validated;*
- *Will the SaMD be withdrawn or will it be only a withdrawal of support for the device;*
- *How sensitive legacy data (patient information, etc.) will be securely stored; and*
- *How the users of the device that is to be decommissioned will be informed and supported.*

In this way both companies can make the appropriate decisions to effectively and gracefully plan the decommissioning of their devices.

The concepts presented in this section relate to clauses 4.2, 7, *and* 7.5.1.1 *in ISO 13485:2003.*

Appendix A: Mapping Medical Device Regulations to IMDRF/SaMD WG/N23

The following table provides a mapping of applicable clauses, articles, and subsections of the regulations for a QMS for SaMD for the jurisdictions represented in the current IMDRF SaMD WG members. It is important to note that not all jurisdictions may require demonstration of compliance to a QMS for all types of medical devices. Regulatory requirements may also permit exclusions or provide alternative arrangements to be addressed in a QMS. It is the responsibility of the organization to ensure conformity with appropriate jurisdictional regulatory requirements. The objective of this table is to share how QMS requirements map to the elements presented in the IMDRF/SaMD WG/N23 when compliance to a QMS is required in the specified jurisdictions.

Applicability to Health Canada regulations:

- The Medical Devices Regulations require class II, III and IV medical devices to be manufactured (class II) or designed and manufactured (class III & IV) under CAN/CSA ISO 13485:2003.

Applicability to Europe Union regulations:

- EU legislation foresees the QMS to be assessed by third parties only for certain classes of products.
- EN ISO 13485:2012 Annexes ZA, ZB, ZC specify in detail which parts of the relevant Annexes to Directive 90/385 (Active Implantable Medical Devices (AIMD) Directives 93/42 (Medical Device Directive (MDD) and 98/79 (In Vitro Diagnostic Directive (IVDD) align to clauses of ISO 13485:2012.
- Note: MEDDEV Guidance 2.1/6 Guidelines On The Qualification And Classification Of Stand Alone Software Used In Healthcare Within The Regulatory Framework Of Medical Devices", while not binding, constitutes a significant additional reference.

Applicability to Australian regulations:

- The *Therapeutic Goods (Medical Devices) Regulations* 2002 require manufacturers to demonstrate compliance with appropriate conformity assessment procedures as specified in Division 3.2, three of which require implementation of a QMS.
- The *Conformity assessment standards order (standard for quality management systems and quality assurance techniques) 2008* enables the use of ISO13485 to demonstrate compliance with applicable clauses of those procedures. Mapping is as per the following table key: [Code]—Procedure name (legislative reference):
    - [P5]—Product Quality Assurance procedures (Schedule 3, Part 5, Clause 5.4)
    - [P4]—Production Quality Assurance procedures (Schedule 3, Part 4, Clause 4.4)
    - [P1]—Full Quality Assurance procedures (Schedule 3, Clause Part 1, 1.4)
    - [All]—required for all (Product, Production, and Full Quality Assurance) conformity assessment procedures
- The # symbol is used to indicate clauses of ISO 13485 considered to additionally be applicable to software medical devices under Australian legislation.

N23	Topic	ISO 13485:2003	Australia	Brazil RDC 16/2013	China MD GMP ([2014]64)	Japan MHLW QMS Ordinance	US 21 CFR
5.0--SAMD QUALITY MANAGEMENT PRINCIPLES	Quality management strategy	4	All	2.1	3,24	5	820.5
	Management responsibility	5			5-7,78		
6.0--SAMD LEADERSHIP AND ORGANIZATIONAL SUPPORT							
6.1--LEADERSHIP AND ACCOUNTABILITY IN THE ORGANIZATION	Management responsibility	5	All				
	Management commitment	5.1		2.2.5, 2.2.6	6	10	820.20b
	Customer focus	5.2				11	
	Quality policy	5.3		2.2.1	6	12	820.20a
	Quality planning	5.4			6	13, 14	820.20d
	Responsibility and authority	5.5		2.2.3	5	15	820.20b1
	Management representative	5.5.2		2.2.5	7	16	820.20b3
	Internal communication	5.5.3		2.2.1		17	
	Management review	5.6		2.2.6	78	18, 19, 20	820.20c
	Internal audit	8.2.2					
6.2--RESOURCE AND INFRASTRUCTURE MANAGEMENT	Resource Management	6	All				
6.2.1--PEOPLE	Provision of resources	6.1	All	2.3	6	21	820.20b2
	Skill management	6.2		2.3	8-10	22, 23	820.25
6.2.2--INFRASTRUCTURE AND WORK ENVIRONMENT	Infrastructure	6.3	All	5.1	12-23	24	820.70f,g
	Work environment	6.4		5.1	11	25	820.70c
7.0--MANAGING SaMD LIFECYCLE SUPPORT PROCESSES							
7.1--PRODUCT PLANNING	Quality planning	5.4	All		6	13	820.20d
	Planning of product realization	7.1	All	4.1	28,29	26	820.30a, 70a
	Design planning	7.3.1	P1	4.1	28,29	30	820.30a,b

N23	Topic	ISO 13485:2003	Australia	Brazil RDC 16/2013	China MD GMP ([2014]64)	Japan MHLW QMS Ordinance	US 21 CFR
7.2--RISK MANAGEMENT: A PATIENT SAFETY FOCUSED PROCESS	Planning of product realization	7.1	All	2.4	4,38	26-5, 26-6	820.30g
7.3--DOCUMENT CONTROL AND RECORDS	Quality system record		All	3.1.6	24		820.186
	Documentation requirements - General	4.2.1			24	6	820.20e
	Quality manual	4.2.2		2.2.1	24	7	820.20e
	Document control	4.2.3		3.1	25,26	8	820.4
	Control of records	4.2.4		3.1.6.2	27	9	820.18
	Device master record			4.2	50	6-2	820.181
7.4--CONFIGURATION MANAGEMENT AND CONTROL	Document control	4.2.3	All	3.1	25,26	8	820.4
	Control of records	4.2.4	All	3.1.6.2	27	9	820.18
	Control of design and development changes	7.3.7	P1	4.1.10	37	36	820.30i
	Production and service provision - General requirements	7.5.1.1	All	5.1	45,46	40	820.70a,g, I,h
	Identification	7.5.3.1	All	6.4	51	47	820.6
	Traceability	7.5.3.2	All	6.4	53	48	820.65
	Status identification	7.5.3.3	All		52	50	820.86
7.5--MEASUREMENT, ANALYSIS AND IMPROVEMENT OF PROCESSES, ACTIVITIES AND PRODUCT	Measurement, analysis, and improvement	8	All				
	Conformity assurance	8.1		2.2.5.1, 2.2.6	78	54	820.8
	Feedback	8.2.1			66	55	
				7.2	71		820.198
				7.2.1.4, 7.2.1.5	75,76		822
	Internal audits	8.2.2		7.3	77	56	820.22
	Process monitoring	8.2.3		7.3, 2.2.6		57	820.70a
	Product monitoring	8.2.4		7.3, 2.2.6	59,60	58	820.8
	Nonconforming product	8.3		6.5	67-70	60	820.9
	Data analysis	8.4		2.2.6, 9	73	61	820.25
	Improvement	8.5					
	Improvement - General	8.5.1		2.2.1	71,76	62	

N23	Topic	ISO 13485:2003	Australia	Brazil RDC 16/2013	China MD GMP ([2014]64)	Japan MHLW QMS Ordinance	US 21 CFR
	Improvement - General	8.5.1		7.2	72,75	62	803
	Corrective action	8.5.2		7.1	74	63	820.1
	Preventive action	8.5.3		7.1	74	64	820.1
	Customer communication	7.2.3		7.2	66,71	29	
	Control of design and development changes	7.3.7	P1	4.1.10			820.70b
	Production and service provision - General requirements	7.5.1.1	All	4.1.11	62		820.184
7.6--MANAGING OUTSOURCED PROCESSES, ACTIVITIES AND PRODUCTS	Purchasing process	7.4	All	2.5	39,40	37	820.5
	Vendor evaluation	7.4.1		2.5.2	41,42	37	820.50a
	Purchasing information	7.4.2		2.5.1	43	38	820.50b
	Verification of purchased product	7.4.3		2.5.4	44		820.8
	Improvement - General	8.5.1		2.2.1	71,76	62	
	Improvement - General	8.5.1		7.2	72 ,75	62	803
8.0--SAMD REALIZATION AND USE PROCESSES							
8.1--REQUIREMENTS MANAGEMENT	Customer requirements capture	7.2.1	All	4.1.3		27	
	Contract review	7.2.2		4.1.6		28	
	Customer communication	7.2.3		7.2	66,71	29	
	Quality system record			3.1.6	24		820.186
	Documentation requirements - General	4.2.1			24	6	820.20e
	Quality manual	4.2.2		2.2.1	24	7	820.20e
	Document control	4.2.3		3.1	25,26	8	820.4
	Control of records	4.2.4		3.1.6.2	27	9	820.18
	Documentation requirements - General	4.2.1		4.2	50	6-2	820.181
	Requirements records	7.1d			24		
8.2--DESIGN + 8.3--DEVELOPMENT	Design and development	7.3	P1				
	Design inputs	7.3.2		4.1.3	30	31	820.30c
	Design and development outputs	7.3.3		4.1.5	31	32	820.30d
	Design and development outputs	7.3.3		4.1.11			820.30j
	Design review	7.3.4		4.1.6	33	33	820.30e
	Design transfer	7.3.1b		4.1.7	32	30-3-2	820.30h
	Control of design and development changes	7.3.7			37	36	

N23	Topic	ISO 13485:2003	Australia	Brazil RDC 16/2013	China MD GMP ([2014]64)	Japan MHLW QMS Ordinance	US 21 CFR
8.4--VERIFICATION AND VALIDATION	Design verification	7.3.5	P1	4.1.4	34	34	820.30f
	Design validation	7.3.6	P1	4.1.8	35,36	35	820.30g
	Verification of purchased product	7.4.3	All	2.5.6	44	39	820.80b
8.5—DEPLOYMENT	Customer communication	7.2.3	All	7.2	66,71	29	
	Production and service provision						
	Contamination control	7.5.1.2.1		6.2.1	48	41	820.70e
	Installation	7.5.1.2.2		8.1	65	42	820.17
	Distribution	7.5.5		6.3	62		820.16
	Servicing	7.5.1.2.3		8.2	64	43	820.2
8.6--MAINTENANCE	Customer communication	7.2.3	All	7.2	66,71	29	
	Production and service provision						
	Servicing	7.5.1.2.3		8.2	64	43	820.2
	Customer property (confidential health information)	7.5.4				51	
	Monitoring & measuring devices	7.6		5.4	56-58	53	820.72
	Feedback	8.2.1			66	55	
8.7--DECOMMISSIONING	Control of records	4.2.4	All	3.1.6	24		820.186
	Documentation requirements - General	4.2.1			24	6	820.20e
	Quality manual	4.2.2		2.2.1	24	7	820.20e
	Document control	4.2.3		3.1	25,26	8	820.4
	Control of records	4.2.4		3.1.6.2	27	9	820.18
	Production and service provision - General requirements	7.5.1.1		4.2	50	6-2	820.181
	Product realization	7					

The following clauses are not specifically addressed in this document:

N23	Topic	ISO 13485:2003 [13, 14]	Australia [15]	Brazil RDC 16/2013	China MD GMP ([2014]64)	Japan MHLW QMS Ordinance	US 21 CFR
These clauses are not specifically addressed by N23	Control of production and service provisions	7.5.1.2	All[#]		47	41	
	Process validation	7.5.2	P1[#], P4[#]		49	45	820.75
	Traceability documentation	7.5.3.2.1	All[#]			48	
	Requirements for active implantable	7.5.3.2.2				49	
	Status identification	7.5.3.3	All[#]			50	
	Device packaging	7.5.5	All[#]		55	52	820.13
	Handling	7.5.5	All[#]		55		820.14
	Storage	7.5.5	All[#]		55		820.15
	Monitoring and measurement	8.2.4.1	All[#]			58	
	Monitoring and measurement of active implantable	8.2.4.2				59	
	Sterilization records	7.5.1.3				44	820.184
	Production personnel						820.70d
	Production and service provision - General requirements	7.5.1.1	P1[#], P4[#]				820.12
	Issue and implementation of advisory notices		All[#]				806
	Medical device tracking						821
	Device classification						860
	Label design						801