SICKNESS RATE
Cardiovascular diseases
Pulmonary disease
Diseases of the digestive system
Liver disease
Diseases of the musculoskeletal system

Congenius Whitepaper

How to develop SaMD | 10 steps

Paul Gardner, Jörg Dogwiler, & Hannah Matthews

Contents

Step 1:

Determine whether your Health Software is SaMD

Step 1 | Determine whether your Health Software is SaMD

What is SaMD?

As health care advances, software has become integrated widely into digital ecosystems that serve both medical and non-medical purposes.

There are three types of software utilised within medical devices:

1. Software **as** a Medical Device (SaMD): Software which **is a medical device**
2. Software **in** a medical device: Software which **is integrated into a medical device**
3. Software used in the **manufacture or maintenance of a medical device**

This whitepaper focusses on type 1 - SaMD.

Step 1 | Determine whether your Health Software is SaMD

The International Medical Device Regulators Forum (IMDRF) defines Software as a Medical Device (SaMD) as:

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

In contrast, software that is driving or influencing the use of a medical device is Software **in** a Medical Device (SiMD) and is covered by the regulations either as a part/component of a device or as an accessory for a medical device. We will not cover SiMD or supporting software in this paper.

Here are some useful notes to help with clarification of the IMDRF definition:

- SaMD is a medical device and includes in-vitro diagnostic (IVD) medical devices
- SaMD can run on general purpose (non-medical purpose) computing platforms
- “…without being part of” means software that does not need a hardware medical device to achieve its intended medical purpose
- Software does not meet the definition of SaMD if its intended purpose is to drive a hardware medical device (accessory to a medical device)
- SaMD may be used in combination (e.g., as a module) with other products including medical devices
- SaMD may be interfaced with other medical devices, including hardware medical devices and other SaMD software, as well as general purpose software
- Mobile apps that meet the definition above are also considered SaMD

Put plainly, think of SaMD as software which is a medical device on its own. For instance, the medical software used to view images from diagnostic equipment on your phone would be SaMD. But the software that enables the diagnostic to run its test would not be. To be considered SaMD, software must not principally drive a hardware device.

Sources:
IMDRF: Software as a Medical Device (SaMD): Key Definitions

Step 1 | Determine whether your Health Software is SaMD

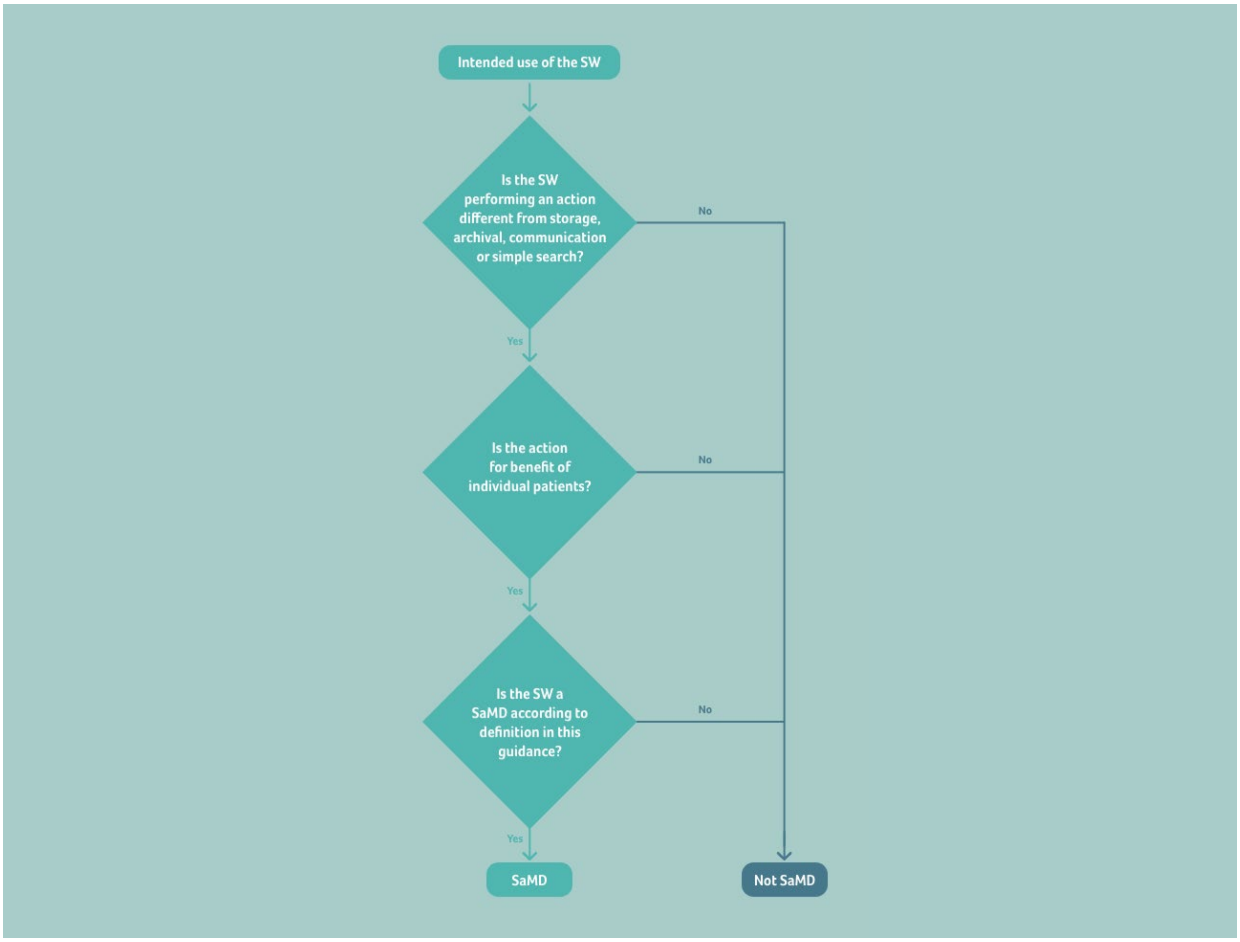
Should my software be classified as a Medical Device?

Software which is intended to process, analyse, create, or modify medical information is qualified as **medical device software,** if the creation or modification of that information is governed by a medical intended purpose.

The software which alters the representation of data for a medical purpose would qualify as a medical device software, e.g., software that searches an image for findings that support a clinical hypothesis as to the diagnosis or evolution of therapy, or software which locally amplifies the contrast of the finding on an image display so that it serves as a decision support or suggests an action to be taken by the user.

However, altering the representation of data for embellishment/cosmetic or compatibility purposes does not readily qualify the software as medical device software.

Furthermore, software intended for non-medical purposes, such as invoicing or staff planning, does not qualify as a medical device software.


Intended use of the SW
Is the SW performing an action different from storage, archival, communication or simple search?
No
Yes
Is the action for benefit of individual patients?
No
Yes
Is the SW a SaMD according to definition in this guidance?
No
Yes
SaMD
Not SaMD

Sources:
FDA: Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act
EU: Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745

My software isn't SaMD, what do I do now?

Where a given product does not fall under the definition of SaMD or is excluded by the scope of the applicable Regulations, other Community and/or national legislation may be applicable. In any case, it is recommended that best practice software development is followed suitable to the risk the software would pose should it fail.

My software is SaMD – what next?

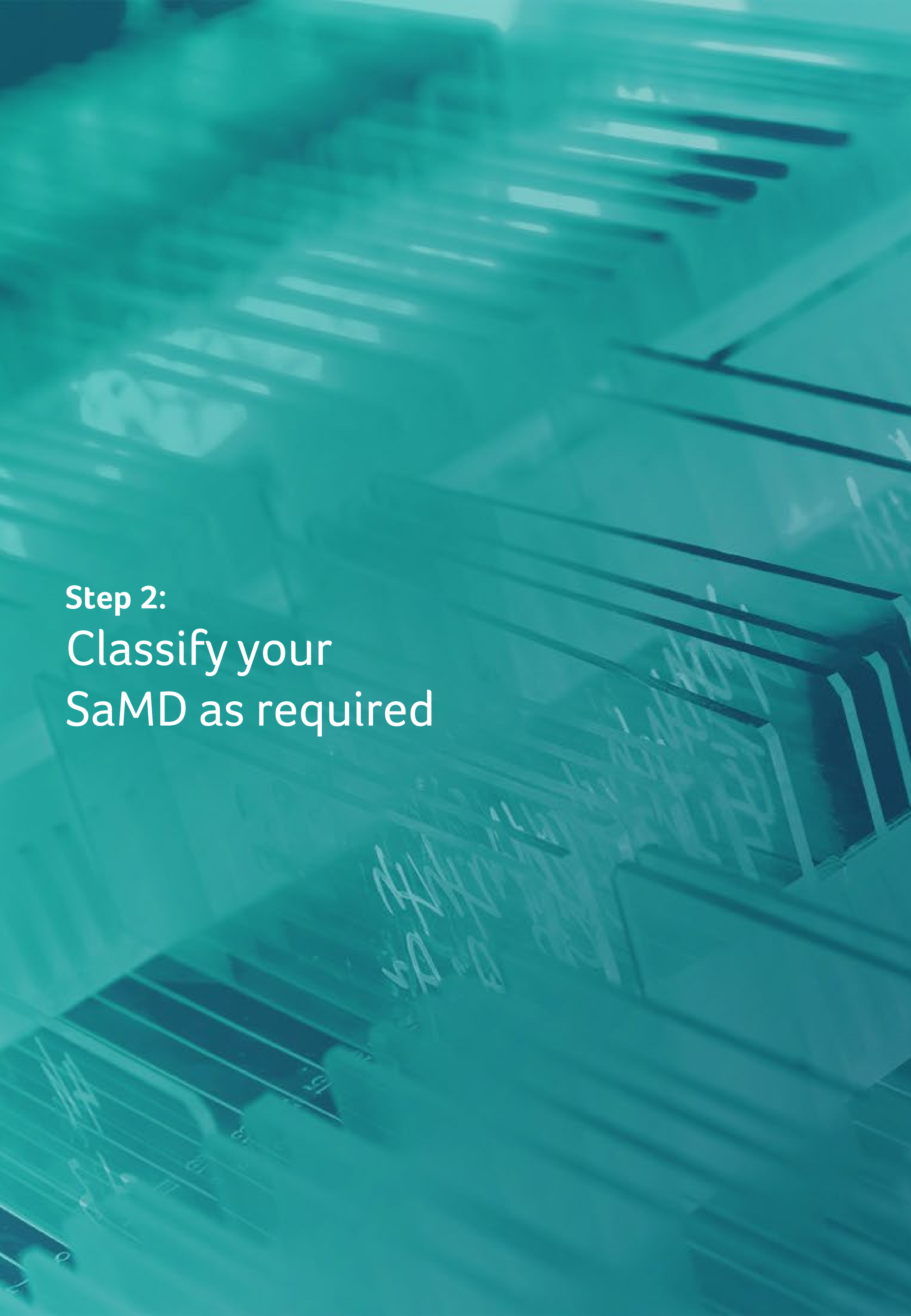
For the EU, you need to classify your SaMD according to MDR 2017/745:

Rule 11 of Annex VIII was introduced into the MDR and is intended to address the risks related to the information provided by an active device, such as SaMD. Rule 11 describes and categorises the significance of the information provided by the active device *(as software is defined as an active device)* to the healthcare decision *(patient management)* in combination with the healthcare situation *(patient condition)*.

For the US, you must classify your SaMD according to IMDRF (FDA) Guidance:

In 2013, IMDRF formed the Software as a Medical Device Working Group (WG) to develop guidance supporting innovation and timely access to safe and effective Software as a Medical Device globally. Chaired by the FDA, the Software as a Medical Device WG agreed upon the framework for risk categorization and subsequent classification for Software as a Medical Devices.

Sources:
EU: Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices
IMDRF (FDA): Framework for risk categorization for Software as a Medical Device



Step 2:

Classify your SaMD as required

Step 2 | Classify your SaMD as required

For the EU:

The EU MDR 2017/745 has **four main categories for Medical Devices classification** defined in Chapter V Section 1 Article 51. The categories cover products with low risk (Class I) to products with high risk (Class III).

Class I

Class I*

- Class Is: A Class I product that is delivered sterile
- Class Im: A product with a measuring function
- Class Ir: A new sub-class for products that are reprocessed

Class IIa

Class IIb

Class III

Step 2 | Classify your SaMD as required

For the EU (continued):

You must define the classification of your device according to **Annex VIII of the Medical Devices Regulation MDR 2017/745**, which defines the following rules for:

- **Rule 1** – Non-invasive devices
- **Rule 2** – Non-invasive devices intended for channelling or storing (which includes cells)
- **Rule 3** – Non-invasive devices that modify biological or chemical composition of blood, body liquids, other liquids, and cells
- **Rule 4** – Non-invasive devices in contact with injured skin or mucous membrane
- **Rule 5** – Devices invasive in body orifices
- **Rule 6** – Surgically invasive devices for transient use
- **Rule 7** – Surgically invasive devices for short term use
- **Rule 8** – Surgically invasive devices for long term use and implantable (including any device administering medicinal products, surgical mesh, or spinal disc)
- **Rule 9** – Active therapeutic devices intended to exchange or administer energy
- **Rule 10** – Active devices for diagnosis & monitoring, emit ionizing radiation
- **Rule 11** – Software intended to provide information which is used to make decisions with diagnosis or therapeutic purposes (from Class I to Class III)
- **Rule 12** – Active devices intended to administer and/or remove medicinal products, body liquids or other substances
- **Rule 13** – All other active devices
- **Rule 14** – Devices incorporating a medicinal substance including human blood or plasma
- **Rule 15** – Contraception or prevention of the transmission of sexually transmitted diseases
- **Rule 16** – Specific disinfecting, cleaning, and rinsing devices
- **Rule 17** – Devices specifically intended for recording of diagnostic images generated by X-ray radiation
- **Rule 18** – Devices utilizing non-viable tissues or cells of human origin or tissues of animal or derivatives
- **Rule 19** – Devices incorporating or consisting of nanomaterial
- **Rule 20** – Invasive devices with respect to body orifices to administer medicinal products by inhalation
- **Rule 21** – Substances or combinations of substances that are intended to be introduced into the human body via a body orifice or applied to the skin and that are absorbed
- **Rule 22** – Active therapeutic devices with an integrated or incorporated diagnostic function which significantly determines the patient management

For SaMD, Rule 11 in particular should be used for classifying your device.

Step 2 | Classify your SaMD as required

For the US:

The FDA has established classifications for approximately 1,700 different generic types of devices and grouped them into 16 medical specialties referred to as panels. Each of these generic types of devices is assigned to **one of three regulatory classes based on the level of control necessary to assure the safety and effectiveness of the device**. The three classes and the requirements which apply to them are:

Class I General Controls

- With Exemptions
- Without Exemptions

Class II General Controls and Special Controls

- With Exemptions
- Without Exemptions

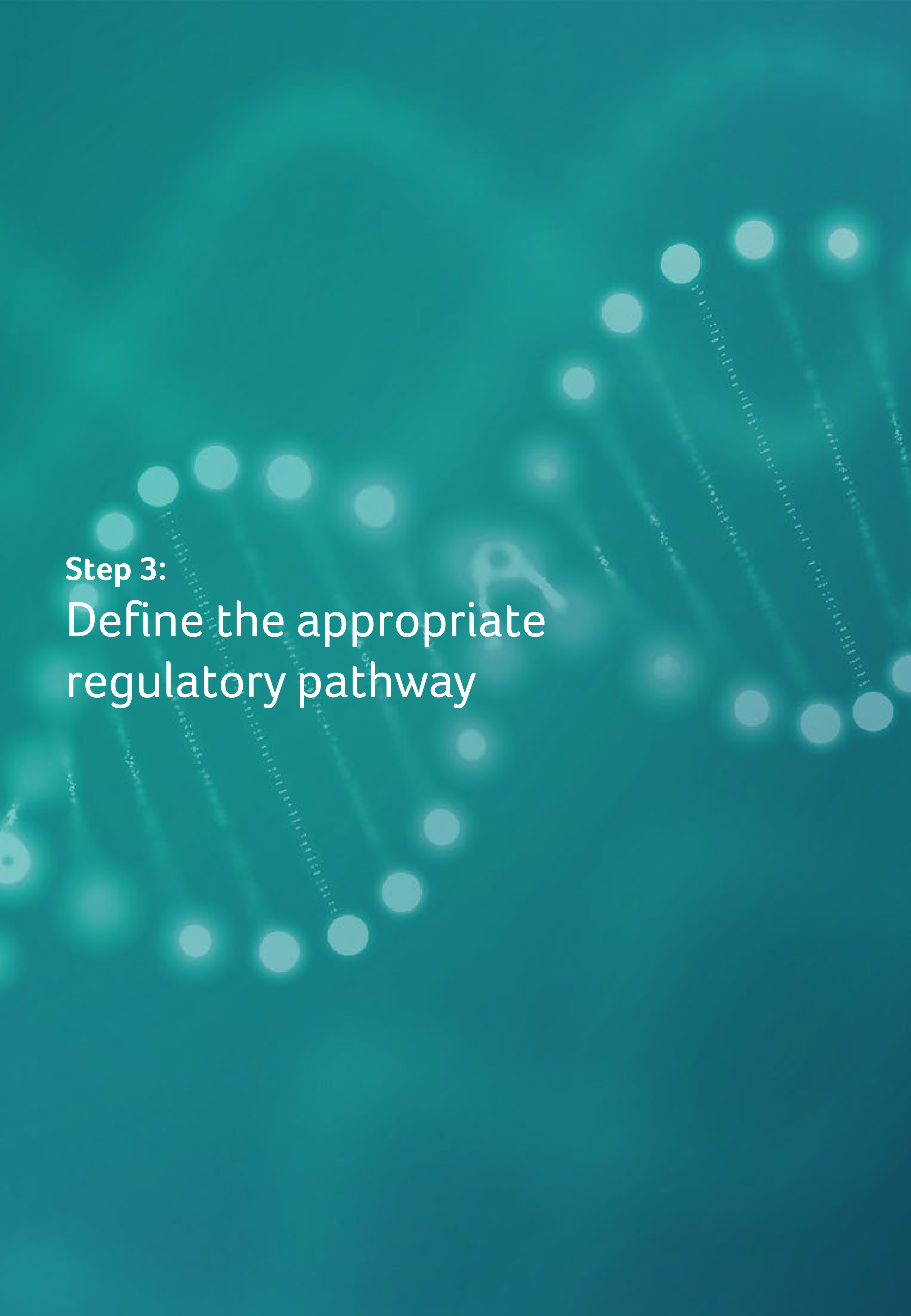
Class III General Controls and Premarket Approval

Finding the classification of your device:

To find the classification of your device, as well as whether any exemptions may exist, you need to find the **regulation number that is the classification regulation for your device**. There are two methods for accomplishing this:

a) go directly to the classification database and search for a part of the device name, or,
b) if you know the device panel (medical specialty) to which your device belongs, go directly to the listing for that panel and identify your device and the corresponding regulation.

If you would like a **formal device determination or classification from the FDA**, consider submitting a 513(g) Request.



Step 3:

Define the appropriate regulatory pathway

Step 3 | Define the appropriate regulatory pathway

Based on the classification of your SaMD, the next step is to choose the regulatory strategy for how to achieve market access for the intended regions.

For the EU:

The conformity assessment based on your device classification is carried out according to Article 52 MDR 2017/745. Prior to placing a device on the market, manufacturers must undertake an assessment of the conformity of that device, in accordance with the applicable conformity assessment procedures set out in **Annexes IX to XI** of MDR 2017/745.

You'll find a useful resource on this here.

For the US:

The device classification regulation defines the regulatory requirements for a general device type. Most Class I devices are exempt from **Premarket Notification 510(k)**, whilst Class II devices require **Premarket Notification 510(k)**, and most Class III devices require **Premarket Approval (PMA).**

Step 4:
Align with the Essential Principles

Step 4 | Align with the Essential Principles

‘Essential Principles’ were widely used for establishing product conformity and are still used in many countries. From a high-level perspective, three basic tenets make up these ‘Essential Principles’:

1. A device must be designed to be safe and perform effectively throughout its lifecycle
2. Device manufacturers must maintain all design characteristics
3. A device must be used in a way that is consistent with how it was designed

How are the Essential Principles specifically implemented in the EU & US?

For the EU:

With the introduction of the EU MDR 2017/745, General Safety and Performance Requirements (GSPRs) are the designated route for establishing conformity with the essential principles. Annex I of the EU MDR 2017/745 details the specific requirements of the GSPR.

GSPRs are broken down into three chapters:

- Chapter 1 - General requirements
- Chapter 2 - Requirements regarding design and manufacture
- Chapter 3 - Requirements regarding the information supplied with the device

For the EU (continued):

The table below details the GSPRs that are applicable to SaMD that meets the definition of a Medical Device.

GSPR	Description	SaMD Applicable?
1	Performance, safety, effectiveness	Y
2	Reduce risks as far as possible	Y
3	Risk management system	Y
4	Risk control measures	Y
5	Use error	Y
6	Lifetime of the device	-
7	Transport and Storage	-
8	Known and foreseeable risks, side effects, benefit-risk	Y
9	Devices listed in Annex XV	-
10	Chemical, physical, and biological properties	-
11	Infection and microbial contamination	-
12	Devices incorporating a substance considered to be a medicinal product	-
13	Devices incorporating materials of biological origin	-
14	Construction of devices and interaction with their environment	Y
15	Devices with a diagnostic or measuring function	Y
16	Protection against radiation	-
17	Electronic programmable systems	Y
18	Active devices and devices connected to them	Y
19	Particular requirements for active implantable devices	-
20	Protection against mechanical and thermal risks	-
21	Protection against the risks posed to the patient or user by supplied energy or substances	-
22	Protection against the risks posed by medical devices intended by the manufacturer for use by lay persons	Y
23	Label and instructions for use	Y

For the US:

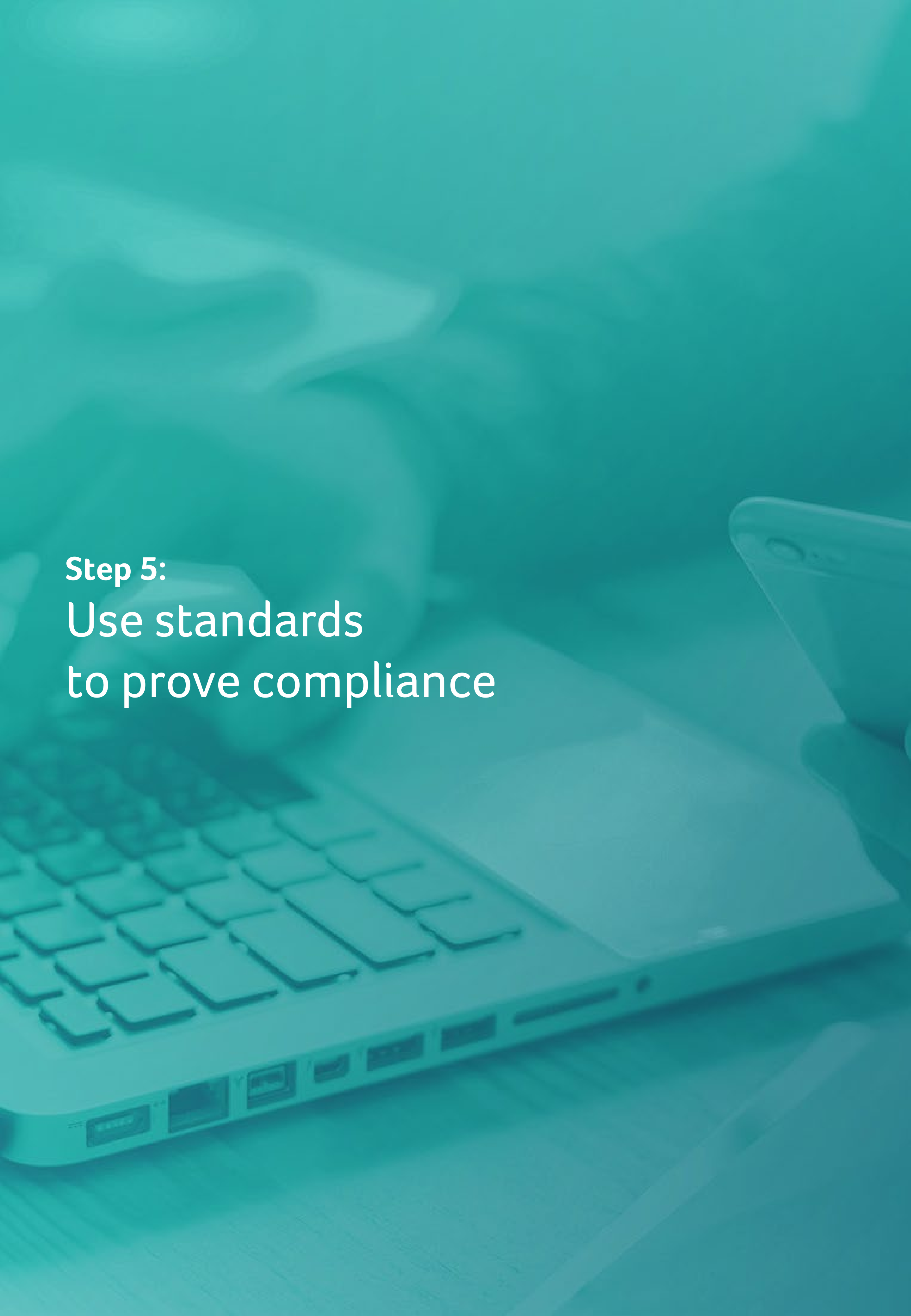
The specific requirements to show compliance to the Essential Principles are dependent on the specific types of premarket submissions:

Premarket Notification (510(k))

A 510(k) is a premarket submission made to the FDA to demonstrate that the device to be marketed is safe and effective, and substantially equivalent to a legally-marketed device that is not subject to Premarket Approval.

Premarket Approval (PMA)

This is the FDA's process of scientific and regulatory review to evaluate the safety and effectiveness of Class III medical devices.



Step 5:
Use standards to prove compliance

Step 5 | Use standards to prove compliance

Manufacturers use standards to prove the compliance of their medical products with the Essential Principles. Standards are documents, written by national or international standardization committees such as ISO and IEC, which document the "state of the art".

For SaMD development, the following standards should be considered in general:

Standard	Description
IEC 82304-1	Health Software – Part 1: General Requirements for product safety
IEC 62304	Medical device software - software lifecycle processes
IEC/TR 80002-1	Guidance on the application of ISO 14971 to medical device software
EN ISO 14971	Application of risk management to medical devices
ISO/IEC 27000	Information Security Management Systems
IEC 62366	Application of usability engineering to medical devices
ISO 15223-1	Symbols for medical device labels, labelling and information to be supplied

For the EU:

European harmonised standards are those that are considered to satisfy the relevant GSPRs specified in the MDR 2017/745. Harmonised standards contain an Appendix Z, that defines which directive the standard meets. Developing to a harmonised standard gives a ‘presumption of conformity’ with the requirements set out in MDR 2017/745.

The list of harmonized standards for SaMD can be found here.

For the US:

Demonstrating conformity with the so-called **FDA-recognised standards** facilitates the premarket review process, including any Premarket Notifications (510(k))s, and Premarket Approval (PMA) applications.

Standards are particularly useful when an FDA-recognised consensus standard exists that serves as a complete performance standard for a specific medical device.

Conformity with other more general standards, e.g., device-specific standards that may not encompass all aspects of device performance, can also streamline the premarket review process.

Step 6:
Operate Controlled Design

Step 6 | Operate Controlled Design

Controlled design involves defining the processes for an approach and practices to ensure a high-quality, risk-based software development process.

The focus of a Software Development Lifecycle (SDLC) is on medical device software development project design controls with the recognition that a quality process contributes directly to higher levels of product safety, productivity, and fewer defects/anomalies in the final product. The SDLC is based on the standard 'Medical device software – Software life cycle processes' according to IEC 62304.

The SDLC is commonly encapsulated in a Standard Operating Procedure in a Quality Management System (QMS) and is intended to provide scalable best practices for medical device software development. For medical device software, the level of activities and required documentation for individual projects depends on the regulatory and safety classification assigned to the software system, with rationale for a separate safety classification for decomposed software items in accordance with IEC 62304.

All medical device software development projects require an approved Software Development Plan (SDP) that defines and justifies the risk-based approach for tailoring the application of design controls defined in this procedure as appropriate for individual projects.

Risk-based Overview

The SDLC defines processes using a risk-based approach and considers the intended use and regulatory classification of the software developed.

The SDLC requires more detailed activities and documents for processes that are of a higher level of criticality and less formal documentation for those items with lower criticality level.

The benefits of applying a risk-based design and development model include:

- More confidence in the safety and security of a developed product
- A greater awareness of the need to design out potential critical defects, and more emphasis on defect prevention practices and failsafe design solutions

It may be useful to utilise a **Secure Product Development Framework** as described in the **latest FDA Cybersecurity guidance**.

Software Safety Classification

For medical device software, a safety classification is assigned as follows:

62304 Software Safety Class	Description	Equivalent FDA Level of Concern
A	The software system cannot contribute to a hazardous situation; or The software system can contribute to a hazardous situation which does not result in unacceptable risk after consideration of risk control measures external to the software system	**Minor** – Failures or latent design flaws are unlikely to cause any injury to patient
B	The software system can contribute to a hazardous situation which results in unacceptable risk after consideration of risk control measures external to the software system and the resulting possible harm is non- serious injury	**Moderate** - Failures or latent design flaws could directly result in injury
C	The software system can contribute to a hazardous situation which results in unacceptable risk after consideration of risk control measures external to the software system and the resulting possible harm is death or serious injury	**Major** - Failures or latent design flaws could result in death or serious injury

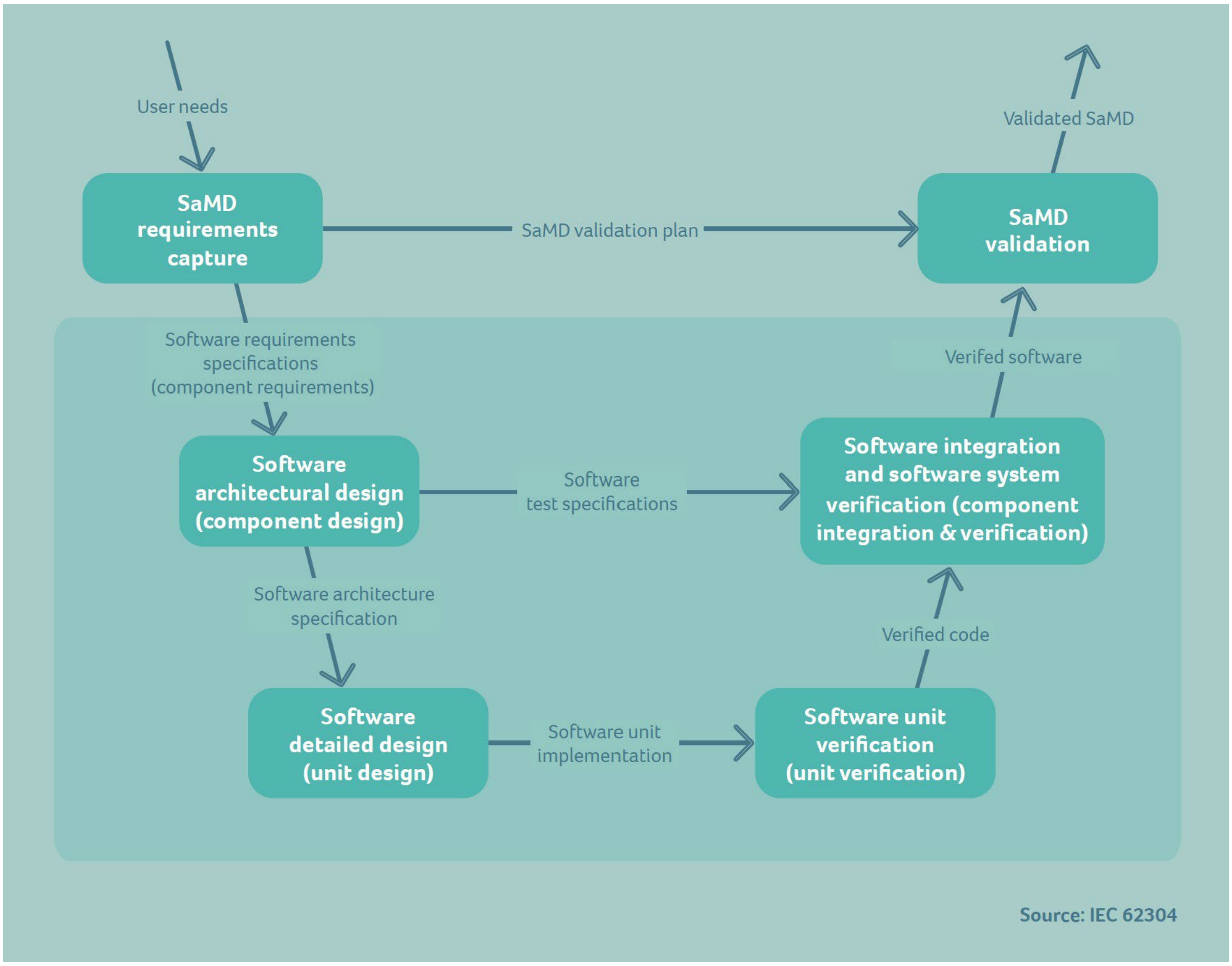
Examples of controls external to the software are hardware, procedures, or other means to minimise that the software can contribute to a hazardous situation.

The safety class of a software system can be reduced by means of external risk control measures. As to the why, this clause assumes that an external risk control is capable of reducing either the consequence or the probability of a failure in such a way that the risk becomes acceptable.

The software safety classification for the system needs to be documented in the Risk Management Plan and the Software Development Plan.

Software Development Methodology

The SDP for a project will define the methodology to be used for a specific project whether this be Waterfall or an iterative methodology like Agile.

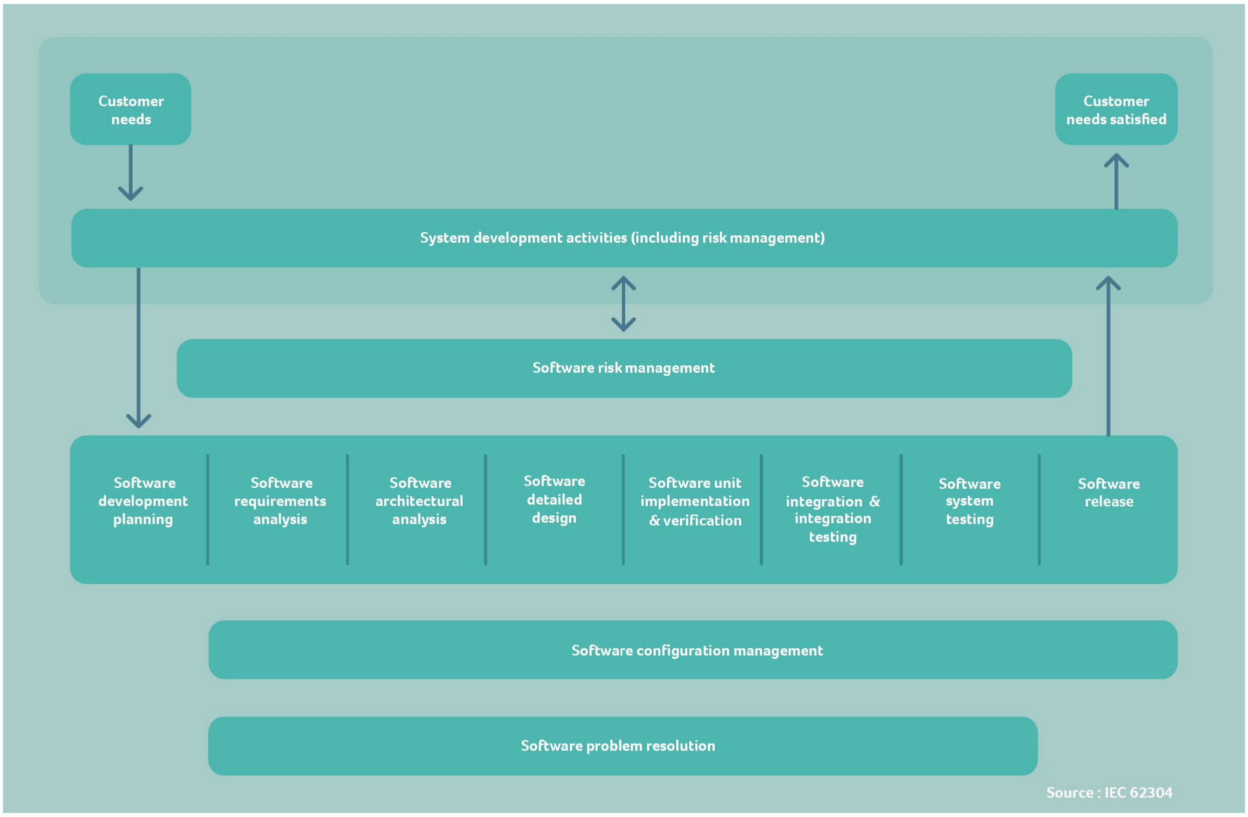

User needs
SaMD requirements capture
SaMD validation plan
SaMD validation
Validated SaMD
Software requirements specifications (component requirements)
Verifed software
Software architectural design (component design)
Software test specifications
Software integration and software system verification (component integration & verification)
Software architecture specification
Verified code
Software detailed design (unit design)
Software unit implementation
Software unit verification (unit verification)

Source: IEC 62304

Software Development Lifecycle

The SDLC consists of a series of phases that are performed incrementally to develop the product and associated documentation. Each phase consists of activities that result in the definition, creation, or update of specified components and deliverable documentation.

The specifics of lifecycle phases may be tailored at the planning level to unique project requirements. Although each phase is presented as a separate section within the SDLC, this is not meant to dictate a strict time sequence relationship. The Software Development Plan for a given project captures the documents required for that project.


Customer needs
Customer needs satisfied
System development activities (including risk management)
Software risk management
Software development planning
Software requirements analysis
Software architectural analysis
Software detailed design
Software unit implementation & verification
Software integration & integration testing
Software system testing
Software release
Software configuration management
Software problem resolution

Source : IEC 62304

Software Design and Development Planning

Plans are developed for software development to:

- identify software design and development activities
- provide the basis for project tracking and control
- show the traceability between system requirements, software requirements, software system test, and risk control measures implemented in software

It is expected that there will be a **Software Development Plan**, a **Risk Management Plan**, a **Verification & (Validation) Plan**, a **Release Plan**, and a **Software Configuration Management Plan**. Depending on the QMS implemented, for low risk, low complexity projects, some (or all) of these items may be included as sections in the Software Development Plan rather than standalone plans.

Software Requirements

Software requirements specifications include functional and non-functional requirements. They provide the basis for the software architecture, software design specifications and software design verification, and include any risk control measures implemented in the software.

Software Architecture and Detailed Design

The Software Architecture Specification establishes a conceptual framework that supports the design and construction of software that satisfies its requirements including those pertaining to security.

The software architecture is segregated into software items and software units. From this decomposition and the design input requirements, a Software Detailed Design Specification (or combined Software Architecture and Detailed Design Specification) is created that elaborates on the information required by developers to implement the software items and software units.

Software Unit Implementation

Software source code is written following established coding guidelines to fulfil software architecture and detailed design specifications. The build outputs from software source code files need to be controlled, and Configuration Management planning is used to describe configuration management and change control for these units.

Software Unit Integration

The software units must be integrated in accordance with the development plan.

Software Design Verification (Integration and System Testing)

Depending on the Software Safety Classification, software design verification activities may include **code reviews**, **unit testing**, **integration testing**, **functional testing**, and **security testing**. The selection of verification activities should be commensurate with the complexity of the software design and the risk associated with the use of the software for the specified intended use.

The criteria for evaluating safety-critical and security-critical aspects of the software should be integrated with the risk management process. As such, the criteria for determining whether additional verification rigor such as code reviews and/or unit tests are required for aspects of the software should be based upon the level of criticality of software risk controls identified in a software FMEA or device hazard/risk analysis for a given project.

Software Release

Configuration management planning describes how software releases are managed. A software release may be done for internal verification and validation testing, external partner testing or as a final production release.

Software Validation

For SaMD, Design Validation needs to take place. It provides test coverage against User Needs Requirements and is covered in Chapter 8 (Consider Usability & Human Factors Engineering) and Chapter 10 (Undertake effective Clinical Evaluation & Post-Market Surveillance) of this paper.

Software Problem Resolution Process

To fully comply with the regulations there needs to be a defined Software Problem Resolution Process. This process must cover handling software anomalies and defects both during the development process and after the SaMD is released to the market (during the Post Market Surveillance Phase).

Software Configuration Management

Software Configuration Management planning may be included in the SDP or a separate plan.

This plan needs to include methods and tools for the control of:

- Internal and External design documentation
- Software source code, resource files, SOUP, and supporting applications

Software Change Control

Changes to released software should be only implemented in response to an approved software change request process. A change request is any documented (and tracked) specification of a change to be made to a software item.

Each software change request needs to be analysed in areas such as technical impact or impact on documentation and severity (safety and security). In addition, the effects of the changes on the currently implemented risk control measures need to be analysed to assure that safety related changes are addressed as a priority.

Phase-Independent Software Development Activities | Off-the-Shelf Software/Software of Unknown Provenance

Off-the-shelf (OTS) Software / Software of Unknown Provenance (SOUP) must be controlled and integrated into products in accordance with established software processes. Where the SOUP functions address safety related requirements, additional review and test activities need to be conducted as appropriate. Thorough testing of normal and fault conditions to assure compliance with established requirements is essential when suitability for use of SOUP cannot be fully established by design test activities including verification and validation.

SOUP components such as operating systems and database systems must be tested in conjunction with the full system application to assure proper performance and a high degree of confidence that no adverse safety related defects exist. Where appropriate, use of SOUP should include an assessment of vendor reported defects and applicability of such defects to applications under development.

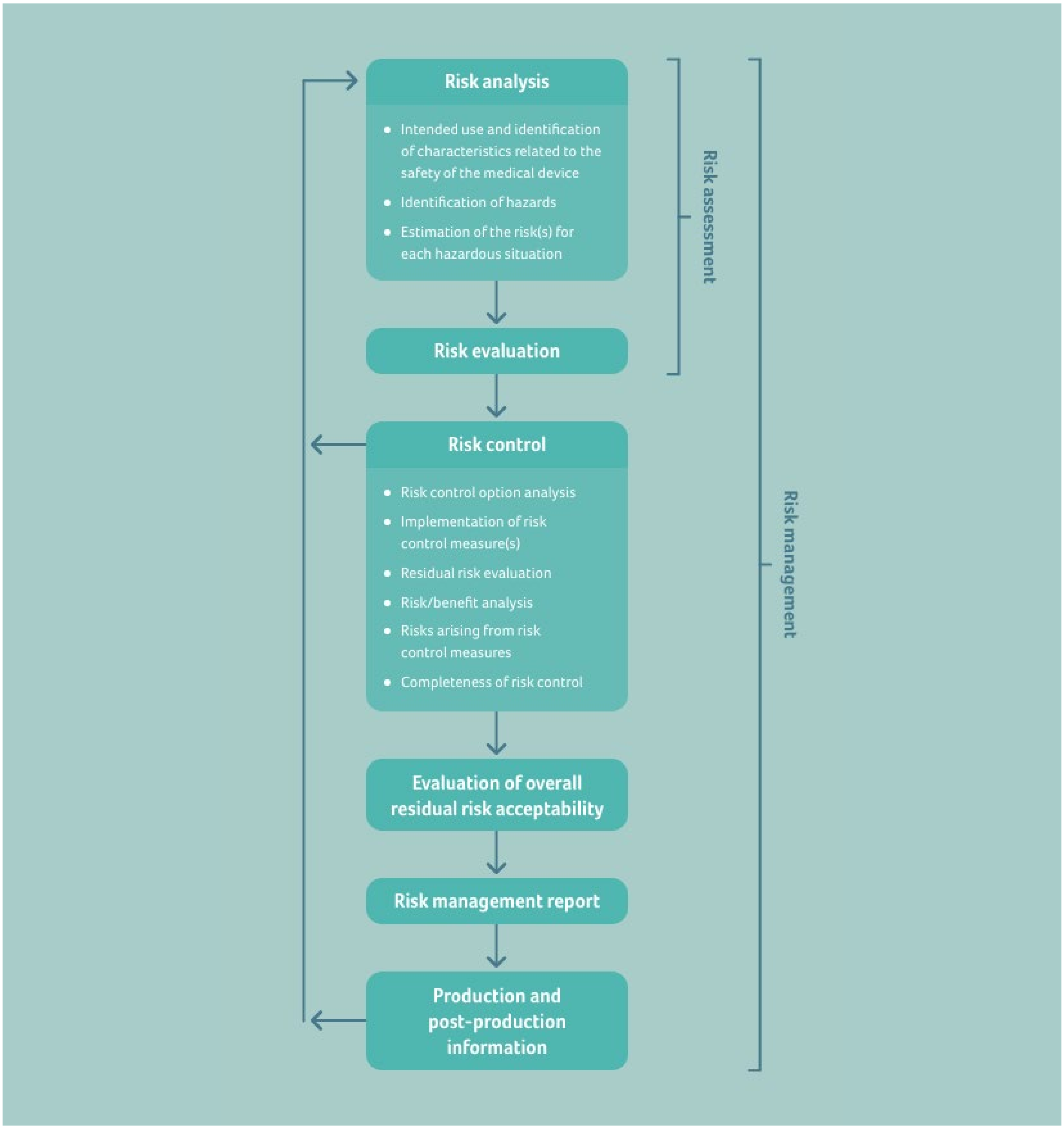
Step 7:

Consider Risk Management for software, cybersecurity & use

Step 7 | Consider Risk Management for software, cybersecurity & use

Risk management involves **identifying, understanding, controlling, and preventing failures that can result in hazards when medical devices are used** and is based on the standard 'Medical devices - Application of risk management to medical devices' ISO 14971.

Manufacturers are expected to identify possible hazards associated with the design in both normal and fault conditions. The risks associated with the hazards, including those resulting from user error, should be calculated in both normal and fault conditions. If any risk is judged unacceptable, it should be reduced to acceptable levels by appropriate means.



Risk analysis

- Intended use and identification of characteristics related to the safety of the medical device
- Identification of hazards
- Estimation of the risk(s) for each hazardous situation

Risk evaluation

Risk control

- Risk control option analysis
- Implementation of risk control measure(s)
- Residual risk evaluation
- Risk/benefit analysis
- Risks arising from risk control measures
- Completeness of risk control

Evaluation of overall residual risk acceptability

Risk management report

Production and post-production information

SaMD's Software related Risk Management

For SaMD Software, a Hazard/Risk analysis is prepared to identify safety risks from Software items including software failures that could cause hazardous conditions. In addition, the Hazard/Risk analysis distinguishes risk estimation for each hazardous situation identified. After evaluating the individual risks, risk control measures to be implemented in the software are defined. If the addition of risk control measures results in new sequences of events leading to hazardous conditions, these are evaluated and documented.

Software failures that could result in hazardous conditions include defects in the implemented software, defects in SOUP (including as found in published anomaly lists), and reasonably foreseeable misuse conditions.

Risk control measures are verified using the appropriate test methods for each risk control measure (and risk).

Risks Related to SaMD Cybersecurity

Design and Implementation

Security threats need to be considered early in the development process. Some of the security activities such as **architecture review**, **threat modelling**, **application security testing**, **penetration testing**, and **risk management** help to reveal the potential vulnerabilities within SaMD.

Design and risk procedures must account for cybersecurity. MDR outlines eight practices for managing the cybersecurity of your device:

1. **Plan and document** all of your security-related activities.
2. **Define your security requirements** in a similar way to your software specifications.
3. **Implement Security by Design.** Your design process should incorporate cybersecurity. "Security by Design" which means designing products to be foundationally secure. It also involves having multiple layers of defence such that the breach of any single element does not compromise the whole system.
4. **Implement your cybersecurity design correctly**, ensuring that any procedures concerning software releases are followed.
5. **Define your Verification and Validation testing activities** and link them to the risk of your software, before then performing validation testing.
6. **Consider Security Breach Management** by documenting how you will handle any security issues should they arise.
7. **Address Change Management** by defining how you would assess risks and roll out software changes.
8. **Provide security guidelines** in user documentation that explain how to operate the medical device with cybersecurity in mind.

Threat Modelling

While the industry standards and best practices help with developing security requirements, you also need to consider the requirements of the product. This is done with a threat modelling exercise, where you consider:

- **Assets:** List the assets to be protected and consider the impact of not having asset protection in place
- **Threats:** Identify threats and their probability
- **Vulnerabilities:** Identify any weaknesses in the system and account for existing countermeasures, if any
- **Risk:** Assess the risk based on the consequences of not protecting assets, the likelihood of the threat, and existing safeguards
- **Priority:** Once the risk is assessed and mitigation is evaluated, prioritise additional mitigations

There are various methods available for threat modelling such as **STRIDE** and **CVSS**.

Security Requirements

One of the key security requirements for SaMD is software integrity/authenticity and data confidentiality. Consider security features such as:

- Secure boot
  - Customer programmable keys
  - Key revocation support
  - Easy access to code signing tools and detailed security documentation
- Secure key storage
- Secure memory

Secure Coding Practices

While this section of our paper mostly focuses on overall security principles, security of your code is an equally critical aspect of SaMD security. Coding guidelines need to include secure coding practices, and code reviews should hold software developers accountable for security.

Software Supply Chain Security

Any brought in source code should be designated as SOUP and vetted to reduce the risk of supply chain attacks.

Security Testing

As with any other medical device testing you should create a Security Test Plan. Security Testing Tools and Penetration Testing are additional testing methods supporting cybersecurity.

Secured Distribution

Finally, the distribution process needs to be secured. Any tools required to release or configure SaMD products need to be controlled.

Laws & Regulations

Various laws have recently been passed to improve the cybersecurity of medical devices, including SaMD.

Americas	EMEA	APAC
• 2021 Executive Order • H.R.1668: IoT Cybersecurity Improvement Act • California SB-327 • Oregon HB 2395 (2019)	• European Cyber Security Act	• Singapore CLS (Cybersecurity Labelling Scheme) • Australia Code of Practice

In the EU, cybersecurity of medical devices is considered part of the General Safety and Performance requirements (GSPR) of the Medical Device Regulation MDR 2017/745. In addition, the General Data Protection Regulation (GDPR) introduces certain data requirements and provides EU-residents with fundamental rights over their data and its protection.

In the US, as part of the software validation and risk analysis required by 21 CFR 820.30(g), software device manufacturers need to establish a cybersecurity vulnerability and management approach. In addition, manufacturers and/or other entities, depending on the facts and circumstances, may be obligated to protect the confidentiality, integrity, and availability of patient information throughout the product lifecycle, in accordance with applicable federal and state laws, including the Health Information Portability and Accountability Act 487 (HIPAA).

Industry standards & guidance

In addition to the legislation, the following guidelines on medical device cybersecurity should be considered when developing SaMD:

For the EU:

- MDCG 2019-16 Guidance on Cybersecurity for medical devices

For the US:

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
- Postmarket Management of Cybersecurity in Medical Devices

Additional Resources

The Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook outlines a framework for health delivery organisations (HDOs) and other stakeholders to plan for and respond to cybersecurity incidents around medical devices, to ensure the effectiveness of devices, and to protect patient safety.

The resources below provide more information on principles for SaMD security and secure coding practices:

- TIR57: Principles for medical device security – Risk management
- IMDRF/CYBER WG/N60FINAL:2020: Principles and Practices for Medical Device Cybersecurity
- OWASP Secure Coding Practices-Quick Reference Guide | OWASP Foundation
- Top 10 Secure Coding Practices – CERT Secure Coding – Confluence

SaMD's Use Related Risk Management

For information on this aspect, see our next chapter (Consider Usability & Human Factors Engineering).

Step 8:

Consider Usability & Human Factors Engineering

Step 8 | Consider Usability & Human Factors Engineering

Define Device Users, Use Environments and User Interface

Prior to conducting use related analysis, you should review and document the essential characteristics of the following:

- Device Users
- Use Environments
- User Interface

Preliminary Analyses and Evaluations

Preliminary analyses and evaluations are performed to identify user tasks, user interface components and use issues early in the design process. These analyses help to focus the Usability Engineering processes on the user interface design as it is being developed so it can be optimised with respect to safe and effective use. One of the most important outcomes of these analyses is comprehensive identification and categorisation of user tasks, leading to a list of critical tasks.

To define this critical task list, a Hazard/Risk analysis is prepared to identify use related risks that could cause hazardous conditions based on the task list of the SaMD. In addition, the Hazard/Risk analysis identifies risk estimation for each hazardous situation identified.

Elimination and Reduction of Use Related Hazards

After evaluating the individual risks, risk control measures to be implemented into the software are defined. If the addition of risk control measures results in new sequences of events leading to hazardous conditions, these are evaluated and documented.

Risk control measures are verified using the appropriate test methods for each risk control measure (and risk).

Human Factors Validation

Human factors validation testing is conducted to demonstrate that the device can be used by the intended users without serious use errors or problems, for the intended uses and under the expected use conditions.

The testing should be comprehensive in scope, adequately sensitive to capture use errors caused by the design of the user interface, and should be performed such that the results can be generalised to actual use.

The human factors validation testing should be designed as follows:

- The test participants should represent the intended (actual) users of the device
- **All critical tasks** must be performed during the test
- The device user interface should represent the final design
- The test conditions should be sufficiently realistic to represent actual conditions of use

Additional Resources

- EU: IEC 62366 'Medical devices – Application of usability engineering to medical devices'
- US: FDA guidance on applying human factors and usability engineering to medical devices

Step 9:

Build up your Technical Documentation (TD)

Step 9 | Build up your Technical Documentation (TD)

The term **technical documentation** refers to the documents that a medical device manufacturer must submit to the authority before placing it on the market. Completing a technical file is an unavoidable step to pass the conformity assessment or approval process by the relevant authorities.

Producing effective Technical Documentation provides manufacturers with their own central information source regarding their medical device. Accurate Technical Documentation can also reduce the review time spent by notified bodies and make an auditor's job significantly easier.

Technical Documentation for the EU:

For a **description of the content** of your EU MDR TD, please refer to MDR 2017/745 as follows:

- Annex II Technical Documentation
- Annex III Technical Documentation on post-market surveillance

For **requirements concerning manufacturers** regarding TD creation, access and maintenance, see:

- Article 10: sections 4 and 8
- Article 11: section 3
- Article 15: section 3b

For the **postmarket surveillance elements of your TD**, see:

- Article 83
- Article 84
- Article 86
- Article 88

A possible structure for your MDR 2017/745 compliant TD can be found here

And for **8 quick tips on producing MDR Technical Documentation**, take a look at our fact sheet here.

Technical Documentation for the US:

The FDA requires detailed technical documentation, comprising three distinct file types:

- Design History File (DHF)
- Device Master Record (DMR)
- Device History Record (DHR)

The **Design History File (DHF)** is a compilation of records which describes the design history of a finished device.

The **Device Master Record (DMR)** is a compilation of records containing the procedures and specifications for a finished device.

The **Device History Record (DHR)** is a compilation of records containing the production history of a finished device.

For an outline of the FDA submission requirements, take a look at the draft guidance on Content of Premarket Submissions for Device Software Functions.

Step 10:

Undertake effective Clinical Evaluation & Post-Market Surveillance

Step 10 | Undertake effective Clinical Evaluation & Post-Market Surveillance

Clinical evaluation is an ongoing process that's conducted throughout the life cycle of a medical device. It is a structured, transparent, iterative, and continuous process that forms part of a device's quality management system.

Whilst Software as a Medical Device (SaMD) is subject to the same general clinical evaluation principles as other medical devices, certain key additions apply.

The General Principles

When it comes to undertaking a clinical evaluation for SaMD, manufacturers must comply with the same legal requirements as for the clinical evaluation of all other types of medical device.

As with other medical devices, SaMD manufacturers specify an intended medical purpose which has a clinical benefit, and therefore, their SaMD requires clinical evidence within its own conformity assessment.

Performing an effective clinical evaluation normally requires clinical data from the device itself. Manufacturers can obtain this clinical data through a clinical investigation, or they can utilise existing data from a proven equivalent product. For SaMD however, this evaluation approach is often not appropriate.

Whether you are producing SaMD for the EU or the US markets, the following three major components should be considered:

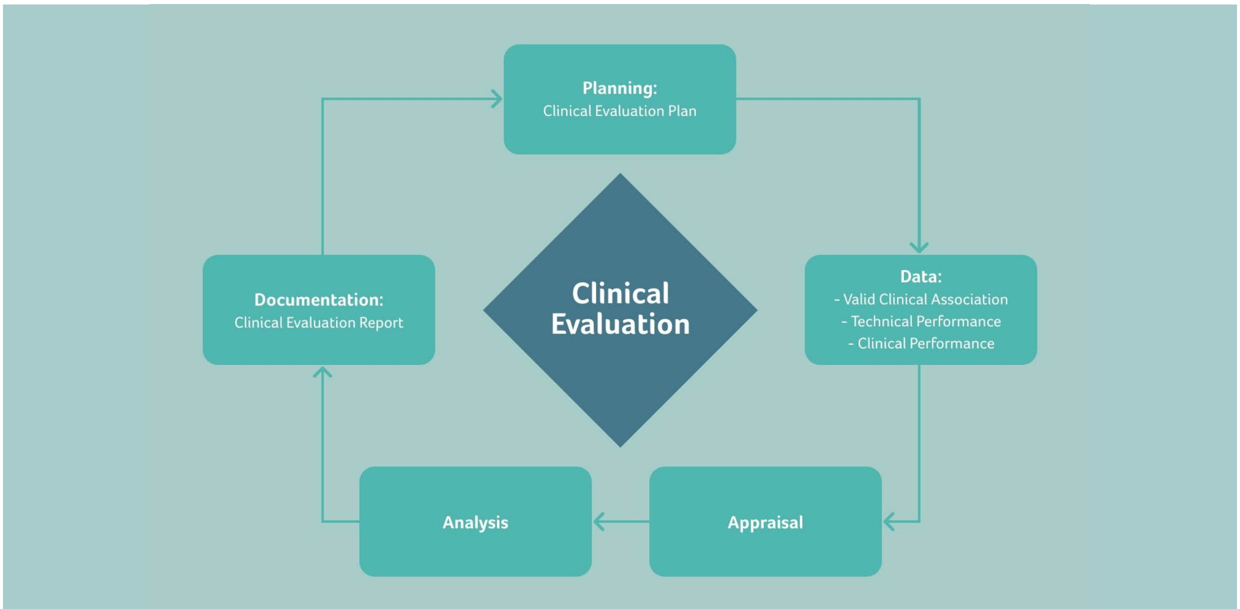
- **Valid Clinical Association** (also known as scientific validity) is used to refer to the extent to which the SaMD's output (concept, conclusion, measurements) is clinically accepted or well-founded
- **Analytical / Technical Validation** is used to demonstrate that the SaMD correctly processes input data, and generates accurate, reliable, and precise output data
- **Clinical Validation** is used to show that using the SaMD's output data achieves the product's intended purpose related to its clinical benefit, and is evaluated and determined by the manufacturer during the development of the SaMD before it is distributed for use (pre-market) and after distribution while the SaMD is in use (post-market)

Requirements for the EU

General Considerations for Medical Devices

The general requirements for clinical evaluation of medical devices are outlined in Article 61 of the MDR 2017/745 (including Annex XIV).

These methodological principles are depicted in the diagram below:



Overview of Clinical Evaluation stages

Specific Considerations for SaMD Clinical Evaluation

The MDCG document **MDCG 2020-1: Guidance on Clinical Evaluation (MDR)/Performance Evaluation (IVDR) of Medical Device Software** outlines a possible alternative path for performing the clinical evaluation for SaMD.

According to the MDCG, three key elements should be considered when compiling clinical evidence for SaMD:

- **Valid Clinical Association**
- **Technical Performance**
- **Clinical Performance**

Valid Clinical Association

Valid clinical association is understood as the extent to which the SaMD's output (e.g., concept, conclusion, calculations), based on the inputs and algorithms selected, is associated with the targeted physiological state or clinical condition. This association should be well-founded or clinically accepted. The valid clinical association of SaMD should demonstrate that it corresponds to the clinical situation, condition, indication or parameter defined in the stated intended purpose.

Evidence supporting valid clinical association can be generated through literature research, professional guidelines, proof of concept studies, or a manufacturer's own clinical investigation studies.

Technical Performance

Technical performance is validated by the demonstration of the SaMD's ability to generate the intended output accurately, reliably, and precisely, from the input data.

Evidence supporting technical performance can be generated:

- Through verification and validation activities such as unit-level, integration, and system testing
- By generating new evidence using curated databases and registries, and reference databases
- By utilising previously collected patient data

Clinical Performance

Clinical performance is validated by the demonstration of the SaMD's ability to yield clinically relevant output in line with the stated intended purpose. The clinical relevance of the SaMD's output is a positive impact:

- on the health of an individual, expressed in terms of measurable, patient-relevant clinical outcomes related to diagnosis, prediction of risk, or treatment response
- related to its function, be that screening, monitoring, or diagnosis
- on patient management or public health

Evidence supporting clinical performance can be generated by testing the SaMD under evaluation, or an equivalent device, with the target population for the intended use. The applied methodology should be appropriate for the device characteristics and intended purpose, and may include pre-clinical testing, a clinical investigation, or a clinical performance study.

Whilst valid clinical association, technical performance, and clinical performance portray a methodological principle for the generation of clinical evidence, they do not represent a distinct stepwise approach.

Determining the Level of Clinical Evidence

To determine and justify the level of clinical evidence, both the amount and quality of supporting data should be evaluated. This assessment can be guided by the following non-exhaustive list of questions:

Sufficient Quantity

- Does the data support the intended use, indications, target groups, clinical claims, and contraindications?
- Have the clinical risks and analytical performance/ clinical performance been investigated?
- Have relevant characteristics of the SaMD, such as the data input and output, the applied algorithms or type of interconnection been considered when generating the data to support the performance of the device?
- What is the grade of innovation/history on the market (how big is the body of scientific evidence)?

Sufficient Quality

- Was the type and the design of the study/test appropriate to meet the research objectives?
- Was the data set appropriate and state of the art?
- Was the statistical approach appropriate to reach a valid conclusion?
- Were all ethical, legal, and regulatory considerations/ requirements considered?
- Is there any conflict of interest?

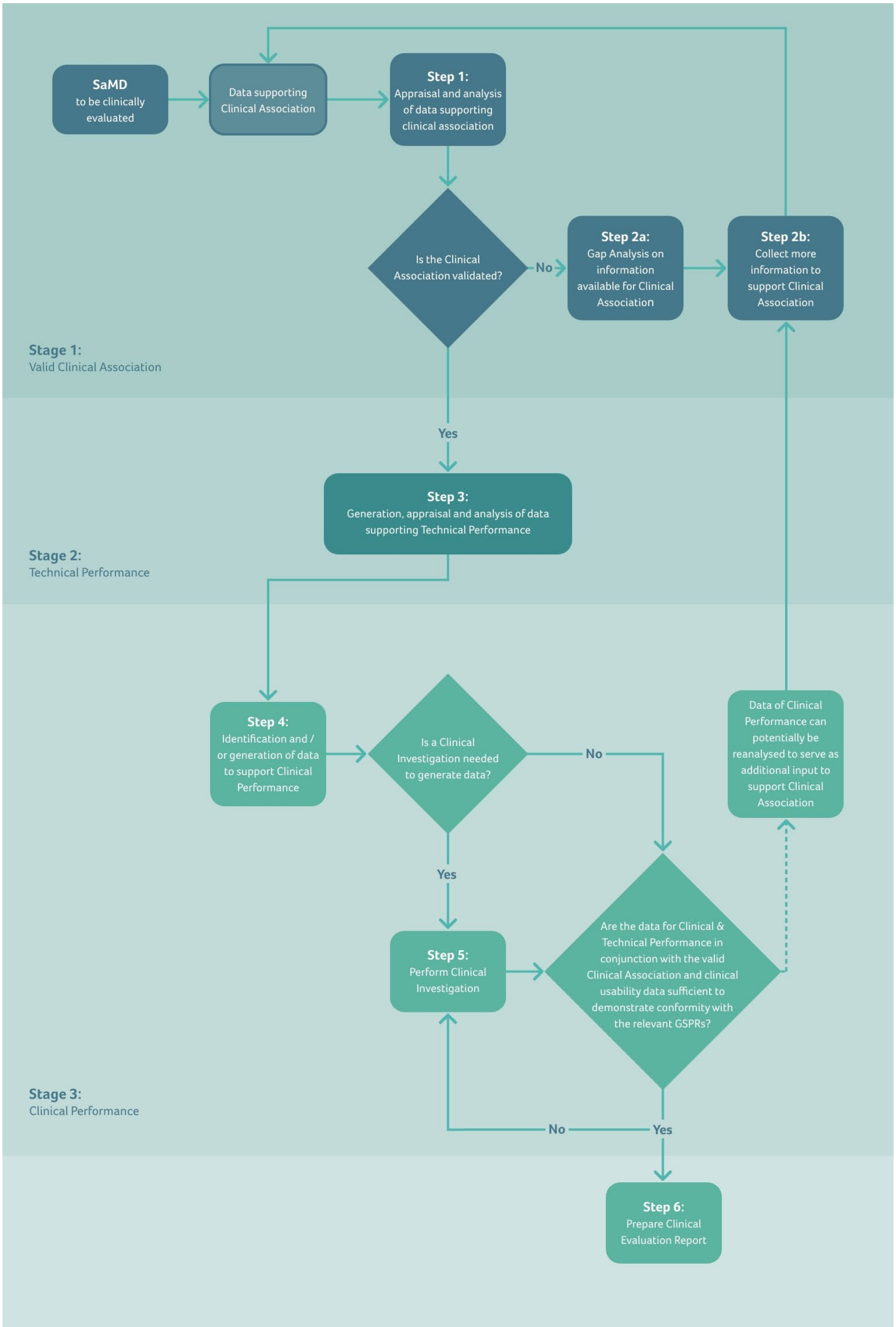
In some cases, particularly for lower risk class I and IIa medical device software (SaMD), clinical data is often not adequate to demonstrate compliance. But both the MDR (Article 61, Section 10) and MDCG document 2020-1 allow an exception.

In such cases, demonstration of compliance with general safety and performance requirements can be based solely on the results of non-clinical test methods including performance evaluation, technical testing (“bench testing”) and pre-clinical evaluation.

However, this must be justified, covered in your risk management, and considered in line with your device’s intended clinical performance.

Step 10 | Undertake effective Clinical Evaluation & Post-Market Surveillance

Methodological Principle for Generation of Clinical Evidence


SaMD to be clinically evaluated
Data supporting Clinical Association
Step 1: Appraisal and analysis of data supporting clinical association
Is the Clinical Association validated?
No
Step 2a: Gap Analysis on information available for Clinical Association
Step 2b: Collect more information to support Clinical Association
Stage 1: Valid Clinical Association
Yes
Step 3: Generation, appraisal and analysis of data supporting Technical Performance
Stage 2: Technical Performance
Step 4: Identification and / or generation of data to support Clinical Performance
Is a Clinical Investigation needed to generate data?
No
Data of Clinical Performance can potentially be reanalysed to serve as additional input to support Clinical Association
Yes
Step 5: Perform Clinical Investigation
Are the data for Clinical & Technical Performance in conjunction with the valid Clinical Association and clinical usability data sufficient to demonstrate conformity with the relevant GSPRs?
Stage 3: Clinical Performance
No
Yes
Step 6: Prepare Clinical Evaluation Report

Overview of methodological principles for Clinical Evidence generation

Putting the Requirements into Practice

Take as an example, SaMD intended for image segmentation. Say a manufacturer develops an independent SaMD intended to allow automatic detection of organs and anatomical structures (such as the aorta) in CT scans with the accuracy of a radiologist.

In this example, the manufacturer claims that the SaMD:

- detects abdominal aortic aneurisms on abdominal CT scans
- detects compression fractures on vertebrae
- detects liver cysts

The following depicts how the three key elements we covered earlier might be realised:

Valid Clinical Association

Method | Literature is reviewed to establish valid clinical association

Evidence | The normal shape and size of anatomy is well established, and the segmentation techniques on cross-sectional images correlates well with the actual size and shape

Result | The valid clinical association is established without any gaps being identified

Technical Performance

Method | Verification and validation tests

Evidence | The basic technical performance such as display, modification, window levelling of images, measurements including confirmation of accuracy, sensitivity, and reliability of the SaMD are as per the expected performance

Result | The technical performance meets the expected performance

Clinical Performance

The undertaking of a usability assessment with the intended user groups, in conjunction with the valid clinical association and validation of technical performance results, is determined as sufficient to demonstrate conformity with relevant GSPRs.

In cases where data is available, a retrospective analysis could be performed. In cases where data does not represent the variability of input parameters, the missing data could be generated in a prospective clinical investigation to establish the clinical performance of the segmentation algorithm.

Continuously Updating your Clinical Evaluation

The safety, effectiveness, and performance of your SaMD should be **actively and continuously monitored**. Such data may include (but is not limited to) post-market information such as complaints, PMCF data, real-world performance data, direct end-user feedback or newly published research / guidelines. The data should be subject to the Clinical Evaluation principles depicted in this chapter's first diagram.

The unique level of connectivity of SaMD facilitates access to **real-world performance data** which can be used for multiple purposes, including, but not limited to:

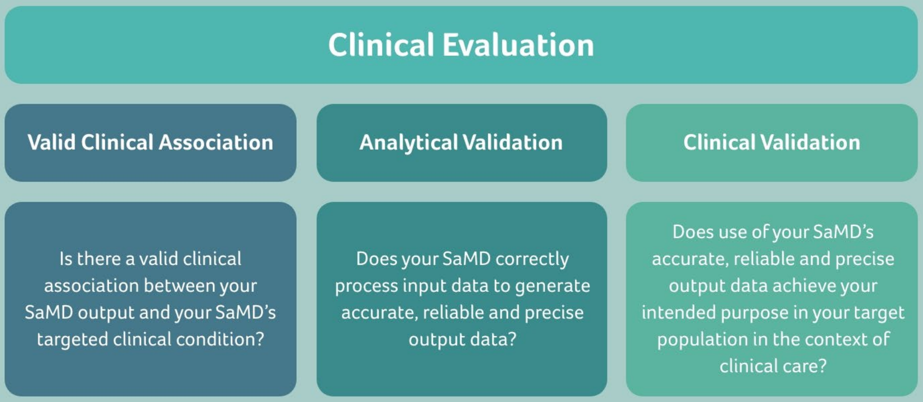
- timely detection and correction of malfunctions
- detection of systematic misuse
- understanding user interactions
- conducting ongoing monitoring of clinical performance
- improving effectiveness
- developing the claims in the clinical development plan
- facilitation of future releases

SaMD can be released for CE marking with initially claimed and validated clinical benefits. Monitoring of real-world performance data can help to formulate hypotheses about future SaMD functionalities and intended uses.

Requirements for the US

Together with the IMDRF, the FDA has published a guidance document that is very similar to MDCG 2020-1-1. Software as a Medical Device: Clinical Evaluation describes a converged approach for planning the process for clinical evaluation of SaMD to establish:

- A valid clinical association between the output of the SaMD and the targeted clinical condition
- That the SaMD yields the expected technical and clinical data



Clinical Evaluation

Valid Clinical Association

Analytical Validation

Clinical Validation

Is there a valid clinical association between your SaMD output and your SaMD's targeted clinical condition?

Does your SaMD correctly process input data to generate accurate, reliable and precise output data?

Does use of your SaMD's accurate, reliable and precise output data achieve your intended purpose in your target population in the context of clinical care?

FDA / IMDRF Clinical Evaluation process

The principle is the same as that proposed by MDCG for the EU. Manufacturers are required to verify the clinical validity of their product with the clinical evaluation of medical device software following the known steps as outlined in our EU section above. In doing so, as the manufacturer, you will effectively demonstrate that the intended purpose is fulfilled and that there are no unacceptable risks.

Congenius

Should you have an SaMD challenge, please do get in touch – our eHealth team is ready and happy to help.

Congenius AG
Riedstrasse 1
CH - 8953 Dietikon

E: info@congenius.ch
T: +41 44 741 04 04

congenius.ch

Revision 1 – July 22