The EU Regulatory Environment of Medical Device Software Development

White Paper

ASPHALION

Introduction

This white paper provides an overview of the regulatory environment in which Medical Device Software (MDSW) should be developed nowadays in Europe, under the new legislative framework given by REGULATION (EU) 2017/745 on medical devices[1] (hereinafter MDR), which will be applicable from the 26th of May, 2021.

This issue is the first of a series that will provide guidance for MDSW developers, regulatory affairs experts, entrepreneurs, and other professionals that might have envisaged to bring new software, that constitutes a medical device (MD) on its own, to the European Union (EU) market. The next issues will address the following subjects:

- MDSW life cycle process according to IEC 62304.
- MDSW Cybersecurity and Safety Risk Management.
- Artificial Intelligence-based MDSW development.

[1] REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

A general overview of MDSW development and the associated standards and guidance

All software that falls under the MD definition provided by this regulation and by its accompanying guidance document, MDCG 2019-11 Qualification and Classification of Software[4], will have to comply with the applicable General Safety and Performance Requirements (GSPRs) listed in Annex I of the MDR.

In order to demonstrate compliance with GSPRs, MDSW legal manufacturers must compile a dossier or technical document (TD) for their product, which includes the contents outlined in Annex II and III of the MDR.

Applicable GSPRs mainly refer to one of the following general fields:

- **Quality Management System (QMS)** requirements
- **Risk Management System (RMS)** requirements
- **Clinical Evaluation** and **Post-market surveillance**[5] requirements
- **Usability** requirements

In addition, these requirements are specifically applicable to MDSW:

- **Software lifecycle** requirements
- **Cybersecurity** requirements

As for any other MD, in order to comply with the applicable GSPRs, it is recommended that MDSW developers apply standardized methods and widely accepted approaches such as the following:

- **International standards** (mainly **ISO**[6], **IEC**[7] and **ANSI/AAMI**[8] standards)
- **MDCG** or **IMDRF** guidance documents

The terms "Software as a Medical Device" (SaMD), primarily used by the IMDRF[2], and "standalone software", used in the medical device directives, refer to software that is intended to be used alone for one or more medical purposes without being part of a hardware medical device, and therefore constituting a device on its own. The MDR and its accompanying guidance documents avoid these terms on the basis that software must be classified depending solely on its intended purpose, regardless of its location (MDCG[3] 2019-11). Since this white paper portrays the EU development environment for software that constitutes a medical device on its own, the term MDSW will be used to refer to this type of software.

[2] IMDRF stands for International Medical Device Regulators Forum.
[3] The MDCG guidance documents are created by the Medical Device Coordination Group.
[4] The MDCG guidance documents are created by the Medical Device Coordination Group. 45 – MDR and Regulation (EU) 2017/746 – IVDR. Note: If the software is mainly intended to process in-vitro diagnostic data, then this software is covered by Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (IVDR), that will come into force in May 2022.
[5] Note: Post-market surveillance is not an integral part of the software development, however, it must be taken into consideration when constructing the Life cycle documentation and the TF.
[6] International Organization for Standardization (ISO)
[7] International Electrotechnical Commission (IEC)
[8] American National Standards Institute (ANSI)/ Association for the Advancement of Medical Instrumentation (AAMI)

Quality Management System (QMS) requirements

MDSW developers must work following a QMS methodology. Although not compulsory for CE- marking, MD manufacturers commonly apply for an ISO 13485[9] certification of their QMS, which could be provided by an MDR-designated Notified Body once the company's QMS has been defined and effectively implemented, and a full audit has been performed.

Risk Management System (RMS) requirements

The main goal of an RMS is to ensure that any potential risks are identified, classified, and reduced without adversely affecting the risk-benefit ratio of the device. For this, the manufacturer must define and implement a risk management plan whereby it duly identifies all risks associated with the device and establishes the corresponding risk mitigation actions that need to be adopted, and assesses their adequacy. This study is normally carried out following ISO 14971 *Medical devices - Application of risk management to medical devices*.

Clinical Evaluation and Post-market surveillance[10] requirements

The clinical evaluation of a MDSW must be carried out following MDCG 2020-1, guidance on Clinical Evaluation of MDSW, and a Clinical Evaluation Report drafted providing the following information:

- A valid clinical association of the software with the targeted clinical condition or physiological state, usually by means of literature references.
- An analytical validation of the software, which demonstrates that the software is capable of correctly processing data.
- And finally, a clinical validation which ensures reliable and precise output from the software within a given clinical context.

Usability requirements

Usability requirements (or human factors engineering) are not specific to MDSW; however, SW developers must ensure that the user interface avoids as many user errors as possible. For this, usability tests must be planned and carried out, in accordance with IEC 62366 *Medical devices — Part 1: Application of usability engineering to medical devices*. All of the identified user errors must be considered in the risk analysis from both a cybersecurity and safety point of view, and thus added to the risk management plan and report. As with any other risk, in case the risk of user-errors cannot be completely eliminated, preventive measures must be adopted such as including training or adding specific warnings in the user manual, among others.

Software lifecycle requirements

The software lifecycle process is described in IEC 62304 *Medical device software — Software life cycle processes*. Note that this standard does not provide guidance on how the stages of SW development must be carried out; however, it does provide a series of steps that should be taken by SW developers. It is the responsibility of the SW developer to define a SW development plan in which it is clearly stated when and how these steps will be taken.

9 EN ISO 13485:2016/AC:2018 (*) Medical devices - Quality management systems - Requirements for regulatory purposes
10 Note: Post-market surveillance is not an integral part of the software development, however, it must be taken into consideration when constructing the Life cycle documentation and the TF.

Cybersecurity requirements

Cybersecurity requirements are explicitly referred to in Annex I of the MDR in relation to MDSW. Nevertheless, other legislations such as the General Data Protection Regulation (GDPR)[11], Network Information Systems (NIS) Directive [12], and the Cybersecurity Act are also applicable. Cybersecurity requirements mainly regard patient data protection and protection from other cyber threats (i.e. hackers compromising the functioning of MD with malicious intent). As for the RMS, an Information Security Management System (ISMS) should be implemented, in which a cybersecurity management plan must be defined and implemented, whereby all related risks are identified and adequate risk mitigation measures established. It is important to consider that cybersecurity risk mitigation measures may create additional safety risks, in which case, these should be taken into consideration in the risk management plan (see above). Therefore, these two aspects of MDSW development are closely interrelated and should be jointly considered.

Due to the above mentioned, the environment of MDSW development is far more complex than that of a typical software lifecycle process. This is depicted in *Figure 1*, where this typical **software lifecycle process** is positioned within the MDSW EU regulated environment, which includes the previously mentioned general and MDSW-specific requirements.

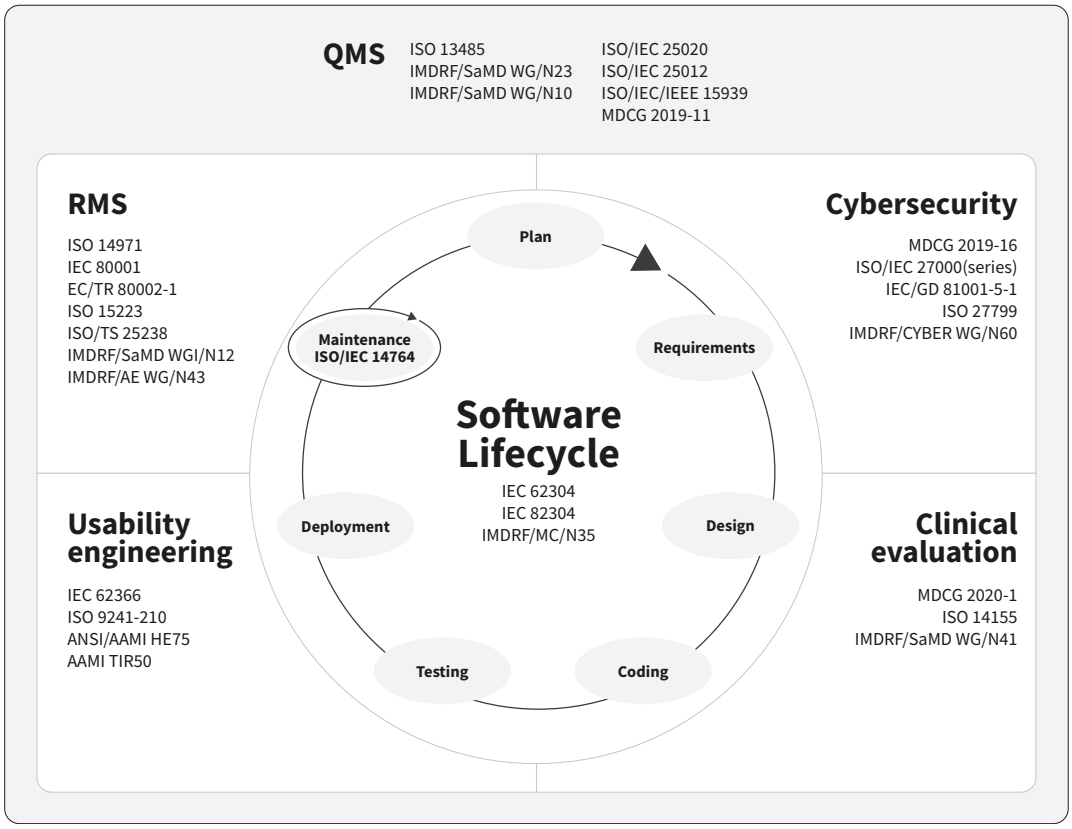

Figure 1 | EU Regulatory Environment for MDSW Development.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[12] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

A comprehensive list of the currently available standards and guidance documents recommended to be followed by MDSW developers to achieve compliance with applicable GSPRs, as well as their latest versions, is shown below:

Requirement	Standard or Guidance	Title
Quality Management System (QMS)	**EN ISO 13485:2016/AC:2018 (*)**	Medical devices - Quality management systems - Requirements for regulatory purposes
	ISO/IEC 25020:2019	Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality measurement framework
	ISO/IEC 25012:2008	Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Data quality model
	ISO/IEC/IEEE 15939:2017	Systems and software engineering — Measurement process
	MDCG 2019-11	Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746
	IMDRF/SaMD WG/N23 FINAL: 2015	Software as a Medical Device (SaMD): Application of Quality Management System
	IMDRF/SaMD WG/N10 FINAL:2013	Software as a Medical Device (SaMD): Key Definitions
Risk Management System (RMS)	**EN ISO 14971:2019 (*)**	Medical devices - Application of risk management to medical devices
	IEC 80001-1:2010 (series)	Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities
	EC/TR 80002-1:2009	Medical device software — Part 1: Guidance on the application of ISO 14971 to medical device software
	ISO/TS 25238:2007	Health informatics — Classification of safety risks from health software
	EN ISO 15223-1:2016 (*)	Medical devices - Symbols to be used with medical device labels, labelling and information to be supplied - Part 1: General requirements
	IMDRF/SaMD WG/N12 FINAL:2014	"Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations
	IMDRF/AE WG/N43 FINAL:2020 & Annexes	IMDRF terminologies for categorized Adverse Event Reporting (AER): terms, terminology structure and codes
Clinical Evaluation	**EN ISO 14155:2020 (*)**	Clinical investigation of medical devices for human subjects - Good clinical practice
	MDCG 2020-1	Guidance on clinical evaluation (MDR) / Performance evaluation (IVDR) of medical device software
	IMDRF/SaMD WG/N41 FINAL:2017	Software as a Medical Device (SaMD): Clinical Evaluation
Cybersecurity	**ISO/IEC 27000:2018(en) (series)**	Information technology — Security techniques — Information security management systems — Overview and vocabulary
	ISO 27799:2016	Health informatics — Information security management in health using ISO/IEC 27002
	IEC/CD 81001-5-1 (draft 2021)	Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product lifecycle
	MDCG 2019-16 rev.1	Guidance on cybersecurity for medical devices
	IMDRF/CYBER WG/N60FINAL:2020	Principles and Practices for Medical Device Cybersecurity
Usability	**IEC 62366-1:2015 (*)**	Medical devices - Application of usability engineering to medical devices
	ISO 9241-210:2010	Ergonomics of human-system interaction - Human-centered design for interactive systems
	ANSI/AAMI HE75:2009/(R)2018 (*)	Human factors engineering- Design of medical devices
	AAMI TIR50:2014 (*)	Post-market surveillance of use error management
Software lifecycle	**EN 62304:2006/AC:2008(*)**	Medical device software - Software life-cycle processes
	IEC 82304-1:2016	Health software — Part 1: General requirements for product safety
	ISO/IEC 14764:2006	Software Engineering — Software Life Cycle Processes — Maintenance
	IMDRF/MC/N35 FINAL:2015	Statement regarding Use of IEC 62304:2006 "Medical device software -- Software life cycle processes"
(*) Although they are not software-specific, these standards are highly relevant for the development of MDSW.		

Table 1 | Standard and guidance documents useful to demonstrate MDSW compliance with MDR.

Documents to keep in sight

The rise of Artificial Intelligence (AI) in MDSW has led to a series of challenges for the industry, especially since regulators have failed to keep up with the evolution of the technology. To deal with these issues, both MDCG and Standard-emitting organizations are currently working on Standards and guidance documents regarding AI.

In 2017, the International Artificial Intelligence Standards Committee Covering the Entire AI Ecosystem, ISO/IEC JTC 1/SC 42 Artificial Intelligence, was created and is presently working on the development of new standards regarding AI, Machine Learning and Big data. To date, this committee has published a single standard regarding AI, ISO/IEC TR 24028:*2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence* (May 2020), and is working on the publication of other documents like the following:

- ISO/IEC WD 5338 *Information technology — Artificial intelligence — AI system life cycle processes*
- ISO/IEC CD 23053.2 *Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)*
- ISO/IEC CD 23894 *Information Technology — Artificial Intelligence — Risk Management*

Although these standards may help AI MDSW manufacturers to cover some of the development areas described in this white paper, they are not specific for MDSW. Therefore, AI MDSW manufacturers must be on the lookout for the publication of the second edition of IEC 62304, *IEC/DIS 62304.2 Health software — Software life cycle processes*, which is now under development and that might address some of the issues they face.

Similarly, the MDCG will publish a guidance: "Artificial Intelligence under MDR/IVDR framework", which will clarify how MDR requirements must be fulfilled for MDSW that includes AI technology.

Another subject that is still unclear to the industry is the legal status of MDSW App manufacturers in the European Economic Area. This is due to the fact that they rely on app stores (i.e. Google Play or IOS App store) for the distribution of their products. In direct response to this uncertainty, the MDCG will publish the "Legal status of app providers" guidance, which is expected to be published in 2020.

Conclusion

MDSW developers must take into consideration all the legal requirements that are applicable to their products. International standards and the MDCG and IMDRF guidance documents must be regarded as the most efficient tools for demonstrating compliance. Identifying the applicable requirements during the development phase and integrating inherent solutions to the design will result in a streamlined NB evaluation of the product, hence avoiding changes to the central code in an attempt of resolving non-conformities.

Asphalion Expertise

Asphalion is an international Scientific and Regulatory Affairs consultancy company, with offices in Barcelona, Madrid, Munich, Amsterdam and London. Founded in 2000, Asphalion has grown consistently, and now employs more than 100 team members from 12 different nationalities with backgrounds in Pharmacy, Chemistry, Biology, Biochemistry, Biotechnology, Medicine, Engineering, and Information Technology.

Asphalion collaborates with Pharmaceutical, Biotechnological and Medical Technology organizations facilitating product development and regulatory affairs solutions for their projects.

Asphalion has extensive knowledge on medical devices and closely monitors every new and movement around the MDR and its accompanying guidance documents in order to be able to better advise and guide manufacturers, developers, regulatory affairs experts, entrepreneurs, and other professionals stakeholders on their implementation.

If you have any questions do not hesitate to contact us!

info@asphalion.com
www.asphalion.com