Getting the Green Light

Regulatory Framework for Software as a Medical Device

GLOSSARY

TERM	DEFINITION
Code of Federal Regulations (CFR) 820	A set of regulations established by the US FDA. Title 21 of the CFR pertains to food and drugs, and Part 820 specifically outlines the Quality System Regulation for medical devices.
European Medicines Agency (EMA)	Agency of the EU responsible for the evaluation and supervision of medicinal products. Its primary role is to ensure the safety, efficacy, and quality of medicines that are intended for use within the European Economic Area (EEA), which includes the EU member states as well as Iceland, Liechtenstein, and Norway.
Food and Drug Administration (FDA)	Federal agency of the United States Department of Health and Human Services (HHS). Its primary responsibility is to protect and promote public health by regulating and supervising various products, including foods, dietary supplements, prescription and over-the-counter medications, vaccines, biopharmaceuticals, blood transfusions, radiation-emitting devices, veterinary products, and medical devices.
IEC 62304	International standard that provides a framework for the software life cycle processes of medical device software.
IEC 62366-1	International standard that provides guidance on the application of usability engineering to medical devices.
In-vitro-Diagnostic Device Regulation (IVDR, (EU) 2017/746)	Regulatory framework established by the EU for in vitro diagnostic (IVD) medical devices. The IVDR replaces the previous In Vitro Diagnostic Directive (IVDD)
International Medical Device Regulators Forum (IproMDRF)	Voluntary association of regulatory authorities from various countries that are involved in the regulation of medical devices. The goal is to promote international convergence and harmonization of regulatory practices related to medical devices.

ISO 13485	International standard that specifies the requirements for a quality management system (QMS) for organizations involved in the design, development, production, installation, and servicing of medical devices and related services.
ISO 14971	International standard that outlines the principles and requirements for the application of risk management to medical devices.
Medical device classes	Medical devices are categorized into different classes based on their potential risk to patients and users. In the European Union, medical devices are classified into four classes, ranging from Class I (lowest risk) to Class III (highest risk).
Medical Device Directive (93/42/EWG, MDD)	Outdated regulatory framework established by the European Union (EU) to regulate medical devices. It was in effect until May 26, 2021.
Medical Device Regulations (MDR, (EU) 2017/745)	Regulatory framework established by the European Union (EU) to govern medical devices. The MDR replaces the previous Medical Device Directive (MDD) and the Active Implantable Medical Devices Directive (AIMDD).
Medical Device Single Audit Program (MDSAP)	Regulatory program that allows for a single audit of a medical device manufacturer's quality management system (QMS) that satisfies the requirements of multiple regulatory authorities. MDSAP was established to streamline and harmonize the audit process for medical device companies selling products in multiple countries.
Notified Body (NB)	Organization designated by a national government within the European Union to assess the conformity of certain products before they are placed on the market.
Software as Medical Device (SaMD)	Software that is intended to be used for medical purposes without being part of a hardware medical device (stand-alone software product).
Software of unknown provenance (SOUP)	Software components from third-party sources or suppliers that are used in a medical device, where the manufacturer does not have complete control or knowledge over the entire software development process.

Introduction

Medical devices play an important role in the healthcare sector. While hardware medical devices make up the majority of devices on the market, software has become an essential part for many devices and a new class of stand-alone software medical devices without any hardware has started to enter the market over the last decade.

In 2008, the first stand-alone software was certified as a medical product by the FDA. [1] While only a few software products were certified as medical devices in the years that followed, approvals have increased steadily since 2016. In 2022, 63 software medical devices were approved. When it comes to the approval of medical devices, strict regulatory requirements must be met, and additional special requirements apply to software. Due to the change in digital technologies, these requirements are constantly being adapted by the regulatory authorities.

In this white paper we give an overview of the complex field of the regulatory framework for medical devices in general and for software in particular. In doing so, we will focus on the requirements and processes of the European Union and the US Food and Drug Administration (FDA) that must be met if you want to bring medical devices to market. We will also examine the unique challenges and considerations involved in developing software as a medical device, including cybersecurity, data privacy, and regulatory harmonization.

By the end of the paper you will have a better understanding of the regulatory framework for software medical devices and their specific requirements.

Regulatory Framework for Medical Devices

Every country has its own medicines agency. This authority regulates the approval of medical devices in the respective country. For the European states there is the European Medicines Agency (EMA). Although each country has its own medical device approval requirements, European states must first meet the requirements of the EMA before their own state requirements are met, the latter usually complementing the European regulations. In the USA, the medicines agency is the Food and Drug Administration (FDA).

The general regulatory framework for medical devices in the European Union are the Medical Device Regulations (MDR, (EU) 2017/745) or the In-vitro-Diagnostic Device Regulation (IVDR, (EU) 2017/746), respectively. MDR focuses on the regulation of medical devices, including devices for in vitro diagnostic (IVD) purposes, but it does not cover all in vitro diagnostic medical devices. IVDR specifically addresses in vitro diagnostic medical devices, which are devices used to perform tests on samples such as blood, urine, or tissue in order to obtain information about the health of a patient.

Both regulations include a comprehensive set of rules for the design, manufacture, and placing on the market of (in vitro diagnostic) medical devices.

The general regulatory framework for medical devices in the USA is Title 21 of the Code of Federal Regulations (CFR) 820. For medical devices that are substantially equivalent to a legally marketed device the 510(k) Premarket Notification is applicable.

Quality Management System

MDR requires a suitable quality management systems (QMS) for manufacturers. Which standard is the most suitable for setting up a quality management system depends on the medical device (e.g. for a class I medical device ISO 9001 certification is sufficient), but ISO 13485 is the only QMS standard that is harmonized to the MDR. [2] This means that this standard, like other standards harmonized with the MDR, is considered preferred by the EU Commission for demonstrating the conformity of a medical product. Manufacturers can also reference other standards but must provide justification for doing so. In addition, ISO 13485 fully covers the requirements described in Art. 10 MDR, which include e.g. the identification of applicable general safety and performance requirements, resource and risk management, clinical evaluation and a post-market surveillance system.

In 21 CFR part 820 QMS requirements are also a very important aspect. The 21 CFR part 820 aligns the QMS requirements according to ISO 13485, however it is not harmonized so far. [3] [4]

ISO 13485 requires a QM manual, including a quality policy and quality objectives, and the documentation of all standard operation procedures (SOP).These SOP must include

- Management responsibility (including management review)
- Resource management (including HR, infrastructure and work environment)
- Product realization (including planning, design and development, purchasing and service provision)
- Measurement, analysis and improvement (including complaint and non-conformity handling and internal audit)

All work done in the company must comply with these SOP. Besides the needed documentation the manufacturer must appoint a quality management officer who ensures that all processes are defined and lived.

All work done in the company must comply with these SOP. Besides the required documentation the manufacturer must appoint a quality management officer who ensures that all processes are defined and lived. [2]

Risk Management

A further central aspect in the regulation of medical devices is risk management. The harmonized standard for risk management to MDR is ISO 14971. Also FDA recognizes ISO 14971 as the underlying standard for risk management. [3]

Before the risk analysis can be conducted, the manufacturer must define the intended use for the medical device. The intended use or intended purpose describes how, on which indications and by whom the product shall be used including all limitations or boundaries. There are several methods for the risk analysis, e.g. FMEA, Fault Tree Analysis or HAZOP analysis, aiming at the identification of all hazards and risks that could arise from the product. In the next step the identified risks need to be assessed, whereby for each risk the severity according to ISO 14971 and the probability of occurrence need to be defined. To determine if a mitigation needs to be implemented to control the considered risk, the manufacturer needs to firstly define criteria for the risk acceptance. This could be done by using a risk acceptance matrix. Manufacturers must reduce the risk as much as possible according to their risk acceptance matrix. All of the mentioned activities need to be documented in a risk management report. After release of the product manufacturers must conduct a post market surveillance. [5]

Usability

MDR and FDA explicitly require that manufacturers identify and control risks that result from a specific context of use and the characteristics of the users (e.g. level of training, intellectual and linguistic skills). This includes

- Suitability to fulfil intended purpose
- Foreseeable misuse
- Elimination or reduction of use errors
- Ergonomics and understandability of displays

In order to provide proof that these requirements have been met, a usability validation is required. IEC 62366-1 and the Human Factors Engineering Guidance document from the FDA reflect the state-of-the-art. But this inspection alone is not sufficient. Manufacturers must conduct a usability study with real users or in a simulated use environment.

IEC 62366-1 requires the specification of users and usage environment, since only representative users are suitable for a usability validation. The number of people, that need to take part in a usability study is not specified in more detail in IEC 62366-1, but it depends on the homogeneity of the target groups. Concrete figures are given in the Human Factors Engineering Guidance document [6]. Here at least 15 participants per user group are required. According to IEC 62366-1, risk-related usage scenarios must be taken into account in the usability validation plan. For this purpose, acceptance criteria must be determined, the aim of which is the correct execution of a task without user errors or difficulties. [7] [8]

Important standards for medical devices:

- MDR/IVDR (EU) and 21 CFR part 820 (USA)
- ISO 13485 (QMS)
- ISO 14971 (Risk Management)
- IEC 62366-1 (Usability)

International Medical Device Regulators Forum (IMDRF) and the Medical Device Single Audit Program (MDSAP)

The International Medical Device Regulators Forum (IMDRF) is a voluntary group of medical device regulators from around the world, including regulatory authorities from North America, Europe, Asia-Pacific, and Latin America, who collaborate to develop and harmonize medical device regulations globally. The main objective is to promote and accelerate international medical device regulatory harmonization and convergence to ensure the safety, effectiveness, and quality of medical devices worldwide.

For that purpose, the IMDRF founded the Medical Device Single Audit Program (MDSAP), a working group that created a single regulatory audit that satisfies the relevant requirements of the regulatory authorities participating in the program. The members are the national regulatory authorities from Australia, Brazil, Canada, Japan and the USA. The European Union is, like the WHO and the UK regulatory authority, one of the so called Official Observers. Observers are non-participating regulatory authorities that take part in meetings, assessments and other activities of the MDSAP meetings but that do not accept MDSAP audit reports as an alternative to national inspections. One reason for the EU to not participate is considered to be the transition from the MDD to the MDR and the associated challenges. A third category in the MDSAP are the Affiliate Members (Argentina, Israel, Korea, Singapore), that are non-participating regulatory authorities that want to engage in the MDSAP. [9] [10]

The FDA accepts MDSAP audit reports as an alternative to regular FDA inspections

Differences and similarities between EU-MDR and FDA

In general, the European and the FDA conformity assessment process are very similar. The requirements regarding the QMS and an increase in control measure with an increase in risk classification, are common elements between both systems. In both cases no notified body is involved for low risk products. However, in the European system the manufacturers themselves declare the conformity for a class I medical device. [11] Also the content of the technical documentation is very similar, only the structure is different (Technical File and Risk Management File vs. Device Master Record, Design History File and Device History Record), and the European system requires, in contrast to FDA, the documentation of the Clinical Evaluation.

Besides the numerous similarities, there are some differences. In the European system there are very clear rules how to classify a medical device in the risk based (classes I/IIa/IIb/III) and the category based classification system (invasive/non-invasive/active/special). In case of disputes, the competent authority, which itself is subject to regular audits, decides. In the US, medical devices are only classified by a risk based system (classes I/II/III) and the classification rules are less strict. The classification of new products according to FDA has a margin of discretion. [12]

Based on 21 CFR part 820 a clinical study is a requirement for the premarket approval. In fact, the leaner 510(k) Notification is used more often, which can be submitted before the manufacturer even has a certified QM system. Products without a full FDA clearance can be put on the market with a 510(k). Whereas in the European system the certification of the QMS and the certificate of conformity is a prerequisite for the selling of medical devices.

Another important difference between the European and the FDA conformity assessment are the Notified Bodies. While in the FDA conformity assessment no Notified Bodies exist (the FDA itself is the responsible entity for the approval

of medical devices in the USA), the EU has designated the Notified Bodies to carry out the conformity assessment and to review the approval of medical devices on behalf of the EU. Using a database from the European Commission can help identify the appropriate Notified Body. [13]

Transition period from MDD to MDR and legacy products

New medical devices can only be certified according to MDR since May 26, 2020. For legacy devices, i.e. products that have been certified under the Medical Device Directive (93/42/EWG, MDD), the legislator requires a transition to MDR. The transition periods for legacy products have been heavily discussed recently. These transition periods were extended due to potential shortages of medical devices, as only a portion of the medical devices currently available in the EU would have had continued authorization by the initial deadline in May 2024.

The length of the transition period is determined by the risk class. Specifically, the following deadlines apply [12] [14]:

- May 26, 2026: Custom-made medical devices (Class III)
- December 31, 2027: Higher-risk medical devices (non-exempt implants of Class IIb and Class III medical devices)
- December 31, 2028: Medical devices with low risk (Class IIa, Ir, Im, Is)

Legacy products with a valid directive certificate may be placed on the market until the specified deadlines, depending on their risk class.

Attention: The extension of the deadlines is subject to certain conditions, which are listed in Article 120(3)(c) MDR.

SOFTWARE AS MEDICAL DEVICE

What is Software as Medical Device?

While the classification rules for physical products are relatively clear, the qualification of a software in the medical product field can sometimes be difficult. Software in this area is divided into [15]

- software, that is part of a medical device ("embedded software" or "software in a medical device"),
- software that is a medical device itself ("stand-alone software" or "software as medical device"),
- software as accessories of a medical product or
- software that is not a medical device ("health software").

Software as Medical Device (SaMD) can be used on a broad range of technology platforms. According to the definition of a medical device SaMD supports diagnosis or therapy decisions or provides information regarding physiological conditions, illnesses or deformities. [16]

Whether a SaMD should be qualified as medical device depends only on the intended use stated by the manufacturer. A software is a medical device if the manufacturer intends that the software is used for diagnosis, therapy or monitoring of diseases or injuries. In other words, a SaMD is a medical device if the intended use conforms to the definition given in the MDR. The actual function of a SaMD is to be considered secondary when it comes to qualify a SaMD. The decision if a software is qualified as medical device depends on the manufacturer. [15]

Often you can find the term "Medical Device Software". This includes both "embedded software" and "software as a medical device".

Special regulatory requirements for SaMD

Stand-alone software that has an intended use according to the definition given in the EU MDR is classified as active medical device. The risk classification depends on the risks for patient and user posed by the product. The classification rules can be found in the MDR Annex VIII. Besides the standards and norms applicable for medical devices in general, the standards for software development (IEC 62304) and basic safety for medical electrical equipment (EN 60601-1) must be considered for SaMD. Additionally, the two guidance documents for qualification and classification of software (MDCG-2019-11) and for the application of ISO 14971 to medical device software (IEC TR 80002-1:2009) provide further helpful information. On top of that, prior to the development process currently valid state-of-the-art norms and guidance for development, maintenance and validation should be consulted. [17]

IEC 62304 is harmonized under MDR and extends the assessment of the QMS to software development and maintenance, configuration management, risk management, verification, and validation by the manufacturer. It is applicable to the development and maintenance of medical device software, if the software itself is a medical device or an embedded or integral part of a medical device. However, this standard does not cover the validation and final release of the medical device, even if the medical device consists entirely of the software. IEC 62304 requires the implementation of a QMS according to ISO 13485 including software lifecycle processes for the development and maintenance of software for medical devices. [18]

The FDA recognizes IEC 62304 as "Consensus Standard" but does not require conformity. However, the FDA guideline documents contain similar requirements.

The IMDRF has prepared the guidance documents "Software as a Medical Device (SAMD): Clinical Evaluation" and „Software as a Medical Device (SaMD): Application of Quality Management System“. These guidance documents

outline the criteria for assessing the clinical validity of SaMD, including analytical validity, scientific validity, and clinical performance and support manufacturers in implementing a QMS according to ISO 13485. [19]

Protection of patient data

The protection of patient data is a very important aspect that needs to be considered for medical devices, since they can contain a wide range of sensitive information. To protect this data several security features need to be implemented, e.g. encryption, authentication, access control and data security.

The MDR, the GDPR and the FDA CFR require that medical devices meet certain requirements to ensure they are safe, reliable and compliant with data protection regulations. The most important obligations of manufacturers are:

- Implementation of appropriate technical and organizational measures to protect the personal data that is processed when using the device,
- Conduct of a risk analysis,
- Creation of an appropriate data protection concept (compliance with applicable laws and regulations, procedures for the collection, use, storage, transmission, and destruction of personal data),
- Ensuring that data protection requirements are also met by other companies involved in the supply chain and
- Data protection training of all stakeholders who come into contact with medical devices (designers, manufacturers, doctors, nurses and other healthcare professionals).

Cybersecurity

Increasing digitalization and connection of devices offers a lot of opportunities in our daily life and in the healthcare sector. However, this also makes it easier for systems to be compromised by outside attackers, especially since the professionality of the attackers increases. Cybersecurity for medical devices includes on the one hand the functional safety to protect the patient or user against system errors and on the other hand the protection of the machine against humans by preventing attacks from the outside (security). The aim of all measures in both categories is always an acceptable risk level. Cybersecurity must be taken into account at each phase of the product lifecycle.

Cybersecurity cornerstones can be described by the CIA(-A) principle:

- Confidentiality - This includes that personal data or information during storage or transfer is secured and can only be accessed by authorized users.
- Integrity - All data changes are traceable and all documents and repositories are under version control.
- Availability - Stored data must be available and protected against data loss. The functionality of a system must be maintained.
- Authenticity - Authentification can be applied to either information or entities (users or devices). In case of information an authentification refers to the evidence of the secure source of this information and to exclude manipulation occurred during transport of the information (integrity of information). In case of entities the identity of a user or a device is proven unequivocally in the system.

The MDR requests the compliance to IT security in Annex I containing the general safety and performance requirements. The risk analysis should not only cover an intended usage but should include especially those scenarios that lie outside of the intended use.

The cybersecurity standard IEC 81001-5-1 "Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle" deals with how IT security must be considered throughout the software life cycle. The EU is currently planning the harmonization of IEC 81001-5-1 with a target date of May 24, 2024. IEC 81001-5-1 is directed at manufacturers of "Health Software," which encompasses not only medical devices but also other software used in the healthcare sector. The standard covers the entire life cycle of Health Software, from development to post-market surveillance. The general requirements of IEC 81001-5-1 for software include amongst others, the implementation of a suitable QMS including a process for risk management for IT security and some further software development and maintenance processes that partly overlap with those of IEC 62304 but are specifically tailored to Health Software. [20]

The FDA has published some guidance documents containing requirements for the manufacturer quality management system, the required processes and documentation for a premarket submission [21] and cybersecurity for medical devices containing off-the-shelf (OTS) software [22].

To analyze a product systematically regarding cybersecurity risks and vulnerabilities, it is important to prepare a product architecture overview showing all connections and data flows of the system. Each process, memory and data flow must then be analyzed for potential risks that can compromise patient safety, as well as the confidentiality, integrity, and availability of sensitive data, or can lead to financial losses and reputational damage for healthcare providers.

For the analysis several models can be used, like the STRIDE Model, the DREAD Model, PASTA, VAST, Attack Tree or Kill Chain.

In general, medical devices, whether software or not, must fulfil the general safety and performance requirement, as described in Annex I MDR. However, in specific cases, selected information security measures ("controls") may actually contradict the basic requirements. For this reason, there cannot be a

fixed list of "controls" for medical devices. The intended use of the product defined by the manufacturer is always decisive. [23]

The NSA recommends according to their defense-in-depth strategy a cybersecurity approach that uses multiple layers of security for holistic protection. If one layer is breached, the security measures in the other layers may be able to stop the intruder.

Attention: An ISO 27001 certificate does not replace a cybersecurity risk analysis. ISO 27001 is an internationally recognized standard for Information Security Management Systems (ISMS), not for products!

Medical devices with AI

Artificial intelligence, especially machine learning (ML), is used by manufacturers for a wide variety of problems. This includes, among other things, the diagnosis of e.g. infarcts, cancer, heart disease or degenerative diseases using radiological images, ECG or EEG signals as well as dosage calculations for medication. Artificial intelligence can also be used to improve and evaluate signals and to segment tissue, e.g. for radiation planning.

When training ML models, there are three sets of data. How these three datasets are divided must be decided on a case-by-case basis, among other factors, depending on the size of the available data. However, the following division can be used as a rough guideline.

- Training (approx. 70%) → Training of the model
- Test (approx. 20%) → Evaluation of the model performance (bias)
- Validation (approx. 10%) → Optimization of hyperparameters

Especially with small datasets, k-fold cross-validation is recommended, where the available dataset is divided into k equally sized subsets, and training and testing are performed with different combinations of these subsets.

The manufacturer must apply a suitable data management system to separate and trace these data sets. This also includes introducing controls that prevent data leakage.

The model documentation should state what the model's inputs and outputs are, how many layers the model went through, whether specific image processing techniques were used (e.g. resampling, normalization, or grayscale conversion), and should describe the key features of the model. In addition, some statistics should be indicated, e.g. accuracy (proportion of correct predictions to all predictions), precision (proportion of correct positive predictions to all positive predictions), recall (proportion of correct positive predictions to correct positive and false negative predictions) and the F1 score (harmonic mean of precision and recall).

Until now, the EU has lacked a substantial regulatory framework for AI medical devices. In principle, the same standards apply as those mentioned above. Some requirements can be taken from these, which can also be applied to machine learning [24]:

- The development of software for the collection and processing of data, for the labelling as well as for the training and testing of models must be validated,
- Manufacturers must determine and ensure the competence of the people involved
- Manufacturers must precisely characterize the intended users and the intended use environment, as well as the patients including indication and contraindication,
- Manufacturers using software libraries must specify and validate these libraries as SOUP/OTS.

Specifically for AI medical devices, the EU offers the guidance document "Proposal for a Regulation laying down harmonized rules on artificial intelligence" [25]. AI products are divided into risk-free and high-risk products (does not correlate with the risk classes of the MDR), with medical products being automatically classified as high-risk products. AI products must be placed under human supervision, either directly by the manufacturer or in use by the user. In addition, the manufacturer is required to carry out a risk analysis, which must include protection against the entry of impermissible data and a cybersecurity analysis ((EU) 2019/881). The model must be deterministic, reproducible and robust, the latter must be confirmed e.g. by cross validation.

The FDA provides "Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)" as a guideline for AI medical devices, which, however, only applies to stand-alone software [26]. The ideas outlined in the discussion paper leverage practices from current premarket programs, but require manufacturers to make a commitment to transparency and monitoring of the performance of artificial intelligence and machine learning-based software as a medical device in the real world, as well as periodic updates to the FDA regarding the changes implemented as part of the approved Pre-Specifications and Algorithm Change Protocol. The FDA refers to the risk categories of the IMDRF. [27]

With AI products, a distinction is made between adaptive and static ML models. In principle, adaptive algorithms cannot be easily certified as a medical product, since the same input can potentially produce a different output. Here, regular updates on the statistics of the model would have to be obtained from customers (users), which means that the system had to be evaluated repeatedly. In this case, very narrow learning limits should be set and the newly learned model should first be checked before it is released. Static models can always be certified as medical devices. However, these can deteriorate over time due to social developments, since the input can change. Accordingly, it should be regularly checked whether the underlying ground truth is still correct.

Conclusion

The regulatory landscape of medical devices and especially software medical devices is a complex field that is constantly evolving due to social and technological change. Therefore, it is important for manufacturers of digital medical devices to deal with the ever-changing requirements in order to ensure the safety and effectiveness of their medical devices while driving innovation. This also requires close cooperation between manufacturers, healthcare facilities and users in order to enable patients to access suitable medical products and to adapt the products to the special needs of the patients.

We from ImFusion stand as your reliable partner for medical software solutions. Our expertise spans from development in accordance with IEC 62304 standards to providing comprehensive technical documentation for the software we develop. With our dedicated team, we are committed to delivering innovative and high-quality solutions that not only meet regulatory requirements but also align with your specific needs. A summary of the complete technical documentation that we can provide is available in our whitepaper "Ensuring Quality: The Key Elements of Technical Documentation for Medical Devices". Contact us to learn more about how we can assist you in achieving your medical software goals.

LIST OF REFERENCES

[1] Food and Drug Administration, „Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices," 19 Oktober 2023. [Online]. Available: https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices.

[2] Johner Institut, „Qualitätsmanagement & ISO 13485," 2023. [Online]. Available: https://www.johner-institut.de/blog/category/qualitaetsmanagement-iso-13485/.

[3] Medical Device Academy, „Why modernize 21 CFR 820 to ISO 13485?," 10 January 2023. [Online]. Available: https://medicaldeviceacademy.com/modernize-21-cfr-820/.

[4] National Archives And Records Administration, „Part 820 - Quality System Regulation," 29 November 2023. [Online]. Available: https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-820.

[5] Johner Institut, „Risikomanagement & ISO 14971," 2023. [Online]. Available: https://www.johner-institut.de/blog/category/iso-14971-risikomanagement/.

[6] Food and Drug Administration, „Applying Human Factors and Usability Engineering to Medical Devices," 9 June 2018. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/applying-human-factors-and-usability-engineering-medical-devices.

[7] Johner Institut, „Usability Validierung: Konform mit IEC 62366-1 und FDA," 26 July 2021. [Online]. Available: https://www.johner-institut.de/blog/iec-62366-usability/usability-validierung/.

[8] Johner Institut, „Anforderungen der MDR an die Usability," 18 February 2020. [Online]. Available: https://www.johner-institut.de/blog/regulatory-affairs/anforderungen-der-mdr-an-die-usability/.

[9] International Medical Device Regulators Forum (IMDRF), [Online]. Available: https://www.imdrf.org/.

[10] Medical Device Single Audit Program, „MDSAP Affiliate Members Roles and Responsibilities Policy," 2019.

[11] Johner Institut, „Zulassung von Medizinprodukten: Zulassungsverfahren in der EU und USA," 5 June 2023. [Online]. Available: https://www.johner-institut.de/blog/regulatory-affairs/zulassung-medizinprodukte/.

[12] BV Med, „Medizinprodukte-Zulassungsexperte zu Europa vs. USA: "Keine Anhaltspunkte für die Überlegenheit eines Systems"," 26 June 2015. [Online]. Available: https://www.bvmed.de/de/bvmed/presse/pressemeldungen/medizinprodukte-zulassungsexperte-zu-europa-vs.-usa-keine-anhaltspunkte-fuer-die-ueberlegenheit-eines-systems.

[13] European Commission, „Single Market Compliance Space," [Online]. Available: https://webgate.ec.europa.eu/single-market-compliance-space/#/home.

[14] healthcare-in-europe.com, „MDR: Übergangsfristen für Zulassung verlängert," 21 March 2023. [Online]. Available: https://healthcare-in-europe.com/de/news/mdr-uebergangsfrist-zulassung-medizinprodukte.html.

[15] Johner Institut, „Software as Medical Device: Definitions and Classification Aids," 10 December 2015. [Online]. Available: https://www.johner-institute.com/articles/software-iec-62304/software-as-medical-device/.

[16] International Medical Device Regulators Forum, „Software as a Medical Device (SaMD): Key Definitions," 2013.

[17] British Standards Institution, „Software als Medizinprodukt," 2023. [Online]. Available: https://www.bsigroup.com/de-DE/medical-devices/Technologien/software-as-a-medical-device/.

[18] British Standards Institution, „IEC 62304 Standard für Software für Medizinprodukte," 2023. [Online]. Available: https://www.bsigroup.com/de-DE/medical-devices/Unsere-Dienstleistungen/IEC-62304-Software-fur-Medizinprodukte/.

[19] Johner Institut, „IMDRF: International Medical Device Regulators Forum," 24 April 2023. [Online]. Available: https://www.johner-institut.de/blog/regulatory-affairs/imdrf/.

[20] Johner Institut, „IEC 81001-5-1: Die Norm für sichere Health-Software," Johner Institut, 27 March 2023. [Online]. Available: https://www.johner-institut.de/blog/iec-62304-medizinische-software/iec-81001-5-1/. [Zugriff am January 2024].

[21] Food and Drug Administration, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*, 2023.

[22] Food And Drug Administration, *Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*, 2005.

[23] Johner Institut, „Guideline IT Security," 6 December 2018. [Online]. Available: https://www.johner-institut.de/blog/iec-62304-medizinische-software/leitfaden-it-sicherheit-guideline-it-security/.

[24] Johner Institut, „Regulatorische Anforderungen an Medizinprodukte mit Machine Learning," 20 November 2023. [Online]. Available: https://www.johner-institut.de/blog/iec-62304-medizinische-software/regulatorische-anforderungen-an-medizinprodukte-mit-machine-learning/.

[25] European Commission, „Proposal for a Regulation laying down harmonised rules on artificial intelligence," 2021.

[26] Food and Drug Administration, „Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) - Discussion Paper and Request for Feedback," 2019.

[27] Food and Drug Administration, „Artificial Intelligence and Machine Learning in Software as a Medical Device," 2021.

Disclaimer

This white paper is provided for informational purposes only and should not be construed as legal advice. The information contained herein is subject to change without notice and is not guaranteed to be complete, accurate, or up-to-date. The opinions expressed in this white paper are those of the authors and do not necessarily reflect the views of regulatory authorities. ImFusion is not responsible for any errors or omissions in this white paper, nor for any direct, indirect, incidental, consequential, or other damages arising from or in connection with the use of, or reliance upon, this white paper or the information contained herein. Any reference to a specific product, service, or company in this white paper does not constitute an endorsement or recommendation by ImFusion. Users of this white paper are solely responsible for their use of the information contained herein and are encouraged to seek professional advice before taking any action based on the information provided.

Published March 2024

ImFusion GmbH

Agnes-Pockels-Bogen 1
80992 Munich, Germany

Phone: +49 (0)89 4524 6780
info@imfusion.com
www.imfusion.com