Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Guide for app developers, manufacturers and distributors

Practical guidance

Berne, 7 april 2022

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination de la Confédération et des cantons
Centro di competenza e di coordinamento di Confederazione e Cantoni

Legal notice

Additional information and orders:
www.e-health-suisse.ch

The author thanks the International Electrotechnical Commission (IEC) for permission to reproduce information from its international standards. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein.

Purpose and positioning of this document:

The objective is to promote a basic understanding of regulatory issues related to mHealth apps and to provide an overview of key terminology and processes involved in the definition, development and marketing of an app as a medical device.

Table of contents

1 Introduction

1.1 Background

Introduction

The introduction of the smartphone has opened up a new area of software development. Apps on various topics are in demand and are widely used. Many applications are being developed especially for medical and lifestyle topics with a very broad focus. Whenever medical questions and applications are involved, the developer must be sure to research at an early stage whether the app could also be a medical device – and thus require certification. Currently, this question often comes up too late in the design process. For this reason (and also in view of new European regulations on medical devices and in vitro diagnostics), this guide was developed to help distinguish between lifestyle/wellness products and medical devices, and to prepare for and carry out the certification process. In addition to these topics, the guide is also intended to draw attention to topics that go beyond certification (MedDO) – for example, risks associated with the usage of mHealth solutions that must already be taken into account during development (e.g. data protection and security). The guide is intended to sensitise developers, distributors and software/hardware manufacturers to topics that are important for users. Another objective is to create more transparency for end users in the area of mHealth solutions.

1.2 Content and liability

1.2.1 Guide and checklists

The guide is intended to offer practical guidance as to when an app is to be qualified as a medical device, along with the regulatory requirements that must be fulfilled. In addition, the guide points out where risks may exist in development and how an optimal development process can be implemented.

The guide consists of an in-depth chapter on basic principles, followed by four topic-specific chapters. It concludes with a glossary and a list of online resources. A comment column on the right-hand side of each page contains useful links and keywords summarising the text.

Each chapter begins with a brief summary of the key points.

In addition, eight checklists are available that can be used independently of the guide. These checklists are useful for quality

and process assurance. Based on a set of key questions, they can help the developer to create a safe and compliant medical device.

1.2.2 Disclaimer

The authors make no warranty as to the correctness, accuracy, currency, reliability or completeness of the information provided herein. Liability claims against the authors for material or immaterial damages resulting from the use or non-use of the guide are hereby excluded. Liability for references and links to third-party websites is outside the area of responsibility of the creator of this guide. No responsibility is accepted for such websites. Any access to and usage of such websites are at the user's own risk.

1.2.3 Scope

This guide focuses on the regulatory and legal situation in Switzerland. In addition, the European perspective is considered wherever it appears necessary and useful. Other countries (e.g. the US) are not considered.

In terms of products, the guide focuses on mobile apps which, as medical software, are considered to be medical devices.

2 Basic principles

2.1 Brief summary of the key points

Medical devices are defined by law in the Swiss Medical Devices Ordinance (MedDO) and this definition corresponds to that of the European Medical Devices Regulation (MDR). According to this definition, software can also be qualified as a medical device and thus be subject to the legal requirements for safety and performance. The decisive factor is the intended purpose of the software as defined by the manufacturer. In addition to the definition, there are other documents that can be used as a decision-making aid when determining whether software is to be qualified as a medical device (most notably, MDCG 2019-11). Medical devices must comply with the applicable legal requirements and undergo a certification process in order to verify their conformity. This process varies according to the risk class, since the higher the risk class, the more stringent the requirements imposed on the device. In order to verify that a product meets the requirements, standards can be relied upon (in the case of harmonised standards, this is even mandated). Even if software is not considered a medical device according to the legal definition, it is still recommended to fulfil the quality requirements and observe the relevant standards during development. The requirements relating to data protection and security apply to all apps and are mandatory regardless of whether the software is qualified as a medical device.

2.2 What is a medical device?

Definition of medical device

The revised Swiss Medical Devices Ordinance defines medical devices as follows in Article 3:

Medical devices are instruments, apparatus, appliances, software, implants, reagents, materials or other objects:

a. that are intended by their manufacturer for use in human beings;
b. that do not achieve their principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which action can be assisted by such means; and
c. that serve to fulfil one or more of the following specific medical purposes either alone or in combination:
    1. diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
    2. diagnosis, monitoring, treatment, alleviation or compensation of injuries or handicaps,
    3. investigation, replacement or modification of the anatomy or of a physiological or pathological process or condition,
    4. acquisition of information by means of in vitro investigation of samples obtained from the human body, including donated organs, blood or tissue.

Medical devices also include:

a. contraceptive or fertility-enhancing products;
b. items intended specifically to clean, disinfect or sterilise medical devices.

Medical device accessory means any article that is not a medical device in its own right, but which is intended by its manufacturer to be used together with one or more particular medical devices and:

Definition of accessory

a. which makes it possible to use the medical device or devices in accordance with its or their intended purpose; or
b. which specifically and directly supports the medical function of the medical device or devices in line with its or their intended purpose.

Medical device accessories are also subject to the Medical Devices Ordinance.

Medical devices are further subdivided into:

Classical medical devices and IVDs

- classical medical devices → e.g. plasters, dental implants, blood pressure monitors, pacemakers, potentially also an app
- in vitro diagnostic medical devices → e.g. pregnancy tests, urine tests

Swissmedic is the central Swiss supervisory authority for therapeutic products (medical devices, medicinal products, clinical trials). Swissmedic has its main office in Bern. As a federal public-law institution, it is autonomous with respect to its organisation and management and has its own budget.
Swissmedic is attached to the Federal Department of Home Affairs (FDHA) at the policy level. The FDHA concludes a service agreement with Swissmedic each year, elaborating its mandate. The actual service mandate is defined by the Federal Council and is based on the therapeutic products legislation.
N.B. Swissmedic is responsible for surveillance of medical devices. It is not responsible for their certification.

Swissmedic

The Swissmedic website has brief information videos on the following topics:

Information videos from Swissmedic

- “What is a medical device?”
- “How do medical devices come onto the market?”

- “What are the tasks of Swissmedic in the area of medical devices?”

2.3 Legal foundations in Europe

The free movement of goods in Europe (the "new approach") allows fast and simple market access, but it also demands significant individual responsibility on the part of companies. They are solely responsible for conformity and compliance with the general requirements and must be able to provide verification at any time.

At the European level, medical devices are currently regulated by two Regulations:

- Regulation (EU) 2017/745 on Medical Devices
- Regulation (EU) 2017/746 on In Vitro Diagnostic Medical Devices

In May 2017, the new Medical Devices Regulation (MDR) and In Vitro Diagnostic Medical Devices Regulation (IVDR) came into force. The MDR replaced the MDD and AIMD directives on 26 May 2021, while the IVDR will replace the IVDD on 26 May 2022.

2017/745 (MDR)

2017/746 (IVDR)

The new European Medical Devices and IVD Regulations entail major changes and challenges for the economic operators (manufacturers, importers, distributors, etc.). Even devices that have been placed on the market under the old regulatory system will need to be newly certified under MDR and IVDR (no grandfathering). The MDR and IVDR include new classification rules (with a completely new classification system in the case of the IVDR), and the requirements for clinical data, post-market surveillance etc. are significantly increased.
The most important changes include:

- The technical documentation must be prepared in much greater detail.
- All medical devices must have a UDI=Unique Device Identifier.
- Every company must designate a person responsible for regulatory compliance (PRRC) who possesses appropriate expertise in the regulation of medical devices.
- More detailed clinical evaluations are required, and any updates must also include PMS data.

- There are new classification rules in the MDR (e.g. for nanotechnology, software, etc.), as well as a new rule-based classification system in the IVDR.
- The classification of some products is also changing (e.g. many software products are being upgraded from class I to class IIa or higher).

2.4 Legal foundations in Switzerland

The most important legal foundations in Switzerland are as follows:

Therapeutic Products Act, TPA
Medical Devices Ordinance MedDO

- Federal Act on Medicinal Products and Medical Devices
- Medical Devices Ordinance (MedDO)
- the forthcoming Ordinance on In Vitro Diagnostic Medical Devices (IvDO)
- Federal Act on Research involving Human Beings
- Ordinance on Clinical Trials in Human Research

The MedDO has been revised in connection with the introduction of the new rules on medical devices in Europe and has largely been aligned with the MDR. The new MedDO has been in force since 26 May 2021. Large parts of the MedDO refer directly to the MDR and the requirements pertaining to devices and economic operators (manufacturers, importers, distributors, authorised representatives) are very broadly identical to those of the MDR.

In vitro diagnostic medical devices (IVDs) regulated under the old MedDO now receive their own ordinance (IvDO). The IvDO is based on the European IVDR. Until the IvDO comes into force on 26 May 2022, the old MedDO will continue to apply to IVDs.

Switzerland as a third country within the meaning of the MDR

Under the old regulations (European MDD and old Swiss MedDO) Swiss manufacturers had direct access to the European market thanks to bilateral agreements. Medical devices placed on the market in Switzerland could also be marketed in Europe without any further requirements. However, following the introduction of the MDR and the new MedDO, Switzerland is now considered to be a third country within the meaning of the MDR, and access to the European market is now more difficult for Swiss manufacturers. For more information see section **Fehler! Verweisquelle konnte nicht g efunden werden.**.

As a result, medical devices in Switzerland are covered by the MedDO (and, from 26 May 2022, the IvDO). However, this guide primarily refers to the MDR. Since the MedDO and MDR are broadly similar and since the MedDO refers directly to the MDR, this information also applies to the MedDO. Medical devices from Swiss manufacturers that are CE-certified and placed on the market in the EU can also be marketed in Switzerland without restriction.

2.5 When is software a medical device?

Definition

Software can be used for various medical purposes. A distinction is made between *stand-alone software* (qualified as a medical device due to its intended purpose), software which is part of a medical device, and software which is an accessory. If stand-alone software is qualified as a medical device, it belongs to the group of active medical devices.

Apps and stand-alone software

Since the intended purpose is decisive for qualification as a medical device, it is understandable why software and medical apps are to be considered as medical devices and must satisfy the applicable requirements.

Swissmedic leaflet

For example, the following apps are to be qualified as medical devices:

- Apps used for diagnostic purposes (e.g. cardiac rhythm analysis)
- Apps that control a medical device (e.g. volume adjustment for a hearing aid)
- Apps that are used for specific and individual evaluation of patient data and provide therapeutic suggestions (e.g. birth control calendar with individual display)
- Apps that calculate a medication dosage (e.g. suggestions for corrective insulin)

It is not always easy to decide whether stand-alone software should be qualified as a medical device. A leaflet available from Swissmedic can help to make this decision. It clarifies the most important terminology and issues.

MEDDEV

The guidance document MDCG 2019-11 offers the most comprehensive aid for deciding whether stand-alone software is a medical device.

The Medical Device Coordination Group or MDCG is an expert group required by the MDR and IVDR composed of members from all EU Member States. Various working groups of the MDCG create what are known as MDCG guidance documents. Although the MDCG

documents are not legally binding, they do provide guidance and assistance in interpreting the MDR and IVDR.
MDCG 2019-11 provides criteria and examples for the qualification of stand-alone software as a medical device in accordance with the MDR and IVDR (see section **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Products for which it is not clear from the outset whether they are subject to medical devices legislation are known as borderline cases. The European Commission's Classification and Borderline Expert Group has published decisions on borderline cases in its Borderline Manual. Although the decisions in this manual relate only to the MDD and not the MDR, they are still of interest in interpreting the MDR since the definition of a medical device has not changed significantly. The latest version of the manual includes various examples of medical apps to aid decision-making. The Borderline Manual will also continue under the new regulations.

Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices

2.6 What if my software is not a medical device?

If software does not satisfy the definition of a medical device and cannot be qualified as a medical device based on the MDCG flowchart, then it cannot be certified as a medical device.
However, the development processes and standards referred to in this guide still play a major role in the development of a lifestyle/health/wearables app. If a product is developed in accordance with these principles and the important standards such as usability and the software life cycle are taken into account, developers can be sure that their product has passed through all the necessary stages to be deemed safe and reliable. In particular, development in accordance with key recognised standards can play an important role in the marketing of the product.
Furthermore, use of the checklists is an important quality assurance measure, documenting the major steps in the development process.

Not a medical device

2.7 Risk classes for medical devices

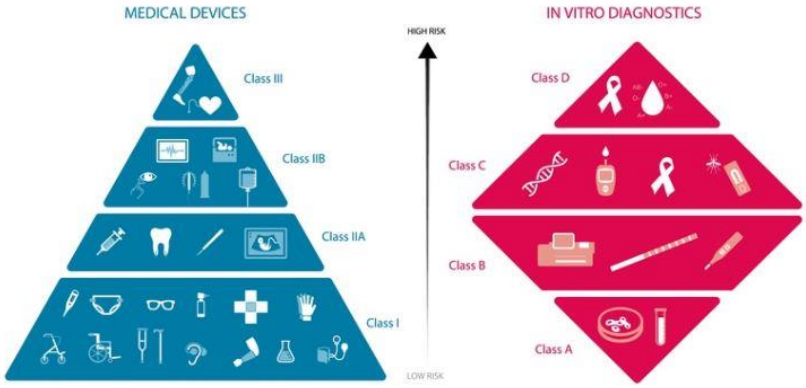


Figure 1 EU MD and IVD risk classes (source: MedTech Europe)

MD risk classes

In Switzerland and Europe, medical devices are divided into four risk classes: classical medical devices fall into Classes I, IIa, IIb and III in accordance with Annex VIII to the MDR; the product information must always be taken into account. Depending on the intended purpose, duration of use and anatomical position of the device, similar devices may be assigned to different classes.

Figure 2 Regulation (EU) 2017/745 on medical devices, Article 51

Risk class	*Class I (low risk)*	*Class IIa (low to medium risk)*	*Class IIb (medium to high risk)*	*Class III (high risk)*
Examples	*Adhesive plasters, corrective glasses*	*Contact lenses, dental fillings, tracheal tubes*	*X-ray devices, urethral stents*	*Cardiovascular catheters, hip, shoulder and knee joint prostheses, pacemakers*

IVD risk classes

Two aspects must be clarified in order to classify IVDs: whether a device is included in List A or List B in Annex II of Directive 98/79/EC, and whether it is intended for self-testing. The new IVDR now has four classes instead of two lists:

Classifi-cation IVDD	*Annex II List A (highly critical IVDs)*	*Annex II List B (critical IVDs)*	*Devices for self-testing*	*Other*
New in IVDR	*D*	*C*	*B*	*A*
Examples	*Blood groups, HIV, hepatitis*	*Infectious diseases, cytomegalovirus, chlamydia*	*Pregnancy test*	*Laboratory device*

Figure 3 Directive 98/79/EC on in vitro diagnostic medical devices Annex II

* the classification under IVDD was also divided into A-D. Although classes A-D still exist in the IVDR, the classification concept has changed fundamentally.

2.8 Certification of medical devices

Notified bodies and conformity assessment

In order to place a medical device on the market, it must comply with all applicable CH and EU regulations and directives and have successfully completed a conformity assessment procedure. Conformity is then indicated visually by a CE mark on the medical device.
In Europe, conformity is tested by so-called “notified bodies”. Notified bodies are independent, authorised third-party entities that carry out conformity assessments on behalf of medical device manufacturers. The manufacturer is free to choose the notified body itself as long as the notified body is accredited by the competent authority in the relevant EEA country or Turkey and has the applicable product group within its scope. Since Switzerland does not have any notified bodies accredited in accordance with MDR, Swiss manufacturers must rely on a notified body in the EU if they wish to place their devices on the European market. CE-marked devices that have been placed on the market in the EU may also be marketed in Switzerland.

Nando
NBOG

Information about notified bodies can be found in the Nando (New Approach Notified and Designated Organisations) information system. The relevant requirements and procedures relating to conformity assessments are specified in various directives and guidelines issued by the EU Notified Body Operations Group (NBOG).

CE self-responsibility

On the manufacturer's own responsibility, the following medical devices are labelled with a CE marking without an identification number:

- Custom-made devices (made specifically for a patient)
- Systems and procedure packs (composed of compliant medical devices and accessories in accordance with the manufacturer's instructions)
- Classical Class I medical devices (non-sterile and without a measuring function)
- Medical devices for in vitro diagnostics, except those listed in Annex II to Directive 98/79/EC (IVDD) and devices for self-testing. Under the forthcoming IVDR, a much larger proportion of IVD devices will need to be certified by a notified body

The manufacturer bears sole responsibility for ensuring that its products comply with the general safety and performance requirements and the applicable CH and EU directives and regulations.

The MDR defines the general safety and performance requirements as all of the minimum requirements that a medical device subject to the directive must fulfil. These essential requirements are specified in Annex I to the MDR. General safety and performance requirements include, for example:

- Risk management to ensure a favourable benefit/risk ratio
- Proof of electrical or mechanical safety
- Usability
- …

CE with notified body

For the following devices, assessment and periodic inspection by a notified body are mandatory:

- Sterile Class I medical devices (Is)
- Class I medical devices with a measuring function (Im)
- Reusable surgical instruments (Ir)
- Class IIa, IIb and III medical devices
- In vitro diagnostic medical devices as defined in Annex II to Directive 98/79/EC (IVDD)
- In vitro diagnostic medical devices for self-testing as defined in Directive 98/79EC (IVDD)
- In vitro diagnostic medical devices in Classes B, C and D according to the forthcoming Regulation (EU) 2017/746 (IVDR)

Depending on the classification and intended purpose of the device, the manufacturer may choose between different certification routes ("conformity assessment procedures").
The procedure to be applied depends on the risk class of the device. In case of uncertainty, it is recommended to discuss the procedure selected with the notified body. As soon as the conformity assessment procedure has been successfully completed, the manufacturer may affix the CE marking to its devices. Depending on the risk class, the identification number of the responsible notified body may also have to be affixed, and the manufacturer receives an appropriate CE certificate. The manufacturer can now place its products on the market in compliance with the regulations.

Conformity assessment procedures

As mentioned, the conformity assessment procedures differ according to the risk class. TÜV SÜD has published an overview of the procedures.

2.9 Relevant standards

Definition of a standard

A standard is a document describing the characteristic properties of a product, process or service. The Swiss Association for Standardization (SNV) cites the definition of this term given in the European standard SN EN 45020:
A standard is a document ... [that] specifies rules, guidelines or properties for general or recurrent use, pertaining to activities or products thereof.

Standards are drafted by national or international standardisation bodies (IEC, ISO, ...) and represent a basic consensus among all interested parties.
In general, a standard is a recommendation and its application is voluntary.

Standardisation (SECO)

Some standards, known as "harmonised standards", are developed by European standardisation organisations (CEN, CENELEC, ETSI) following a request from the EU Commission. EU harmonisation legislation specifies the essential requirements for products to be placed on the market. If a product is manufactured in accordance with the harmonised standards, it is automatically assumed that these essential requirements are fulfilled (presumption of conformity). Harmonised standards are published in the Official Journal of the European Union.

For the MDR, the EU Commission has issued a standardisation request to CEN and Cenelec which lists the standards to be harmonised. To date only a few standards have been harmonised to the MDR. Until harmonisation is concluded, manufacturers can refer to the standardisation mandate to identify applicable standards.

Since it is not always possible to cover all the requirements for a medical device with harmonised standards, national standards can also be applied.
However, if a harmonised standard does exist and it is not applied, the manufacturer must demonstrate that its product fulfils the conditions defined in the essential requirements.
Numerous standards (both national and harmonised) exist for medical devices. In development, special attention must be paid to risk management (ISO 14971) and usability (IEC 62366).
Through appropriate risk management, the manufacturer must, at an early stage, identify the hazards associated with its product, and evaluate and control the associated risks. The risks are evaluated and controlled, and the effectiveness of the controls is monitored, in accordance with defined processes. This procedure increases product safety.
Usability engineering serves, firstly, to make products more user-friendly, e.g. by taking the user's technical knowledge or expertise into account. Secondly, environmental factors and ergonomic properties can be designed so as to minimise the risk of error and make use more user-friendly.

The diagram below illustrates the relationship between the standards and legal requirements:

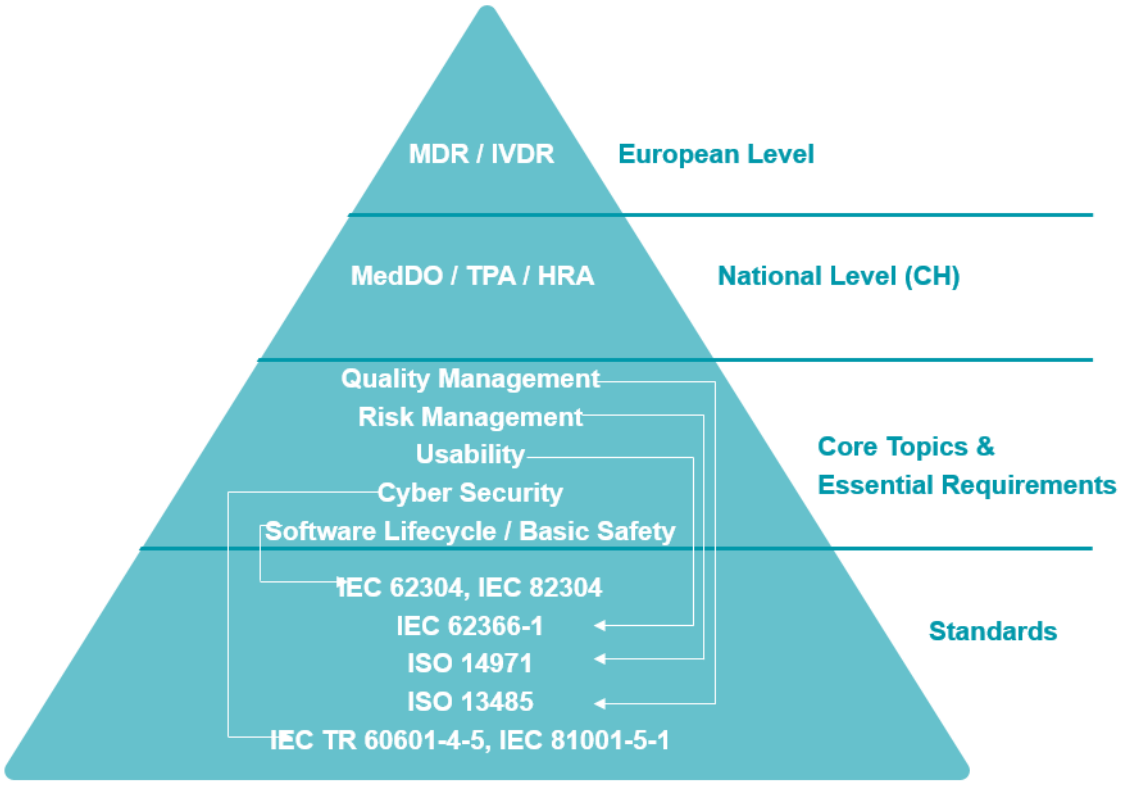


Figure 4: Relationship between standards and regulations (source: ISS AG)

Purchasing standards

Standards are protected by copyright and must be purchased by developers at their own expense. For example, standards can be purchased online from the SNV or from Beuth Verlag.

Standards are regularly revised. New versions may contain fundamental changes to the requirements. For this reason, it is important to monitor the standards used for development. When changes occur, a gap analysis is essential since amendments may trigger a new software release, for example.

2.9.1 ISO 13485:2016 Medical devices – Quality management systems – Requirements for regulatory purposes

ISO 13485, quality management systems

ISO 13485 specifies requirements for a quality management system specifically for medical devices. It represents a specific version of the ISO 9001 quality management standard. ISO 13485 specifies all the requirements that a medical device company's quality management must fulfil in order to ensure safe and reliable medical devices. Certification is performed by a notified body. All medical device manufacturers (with the exception of Class I device manufacturers) require ISO 13485 certification in order to place medical devices on the European market (part of the conformity assessment procedure).

2.9.2 IEC 62304:2006/AMD 1:2015 Medical device software – Software life cycle processes – Amendment 1

IEC 62304 software life cycle processes

This standard specifies requirements for medical device software life cycle processes (development, maintenance, problem resolution, risk management). It was originally developed for software which is part of a medical device (embedded software). In conjunction with IEC 82304, it is also applicable to software which is in itself a medical device (stand-alone software). IEC 62304 is also applicable to mobile medical apps.

The software development process makes up an important part of the standard:

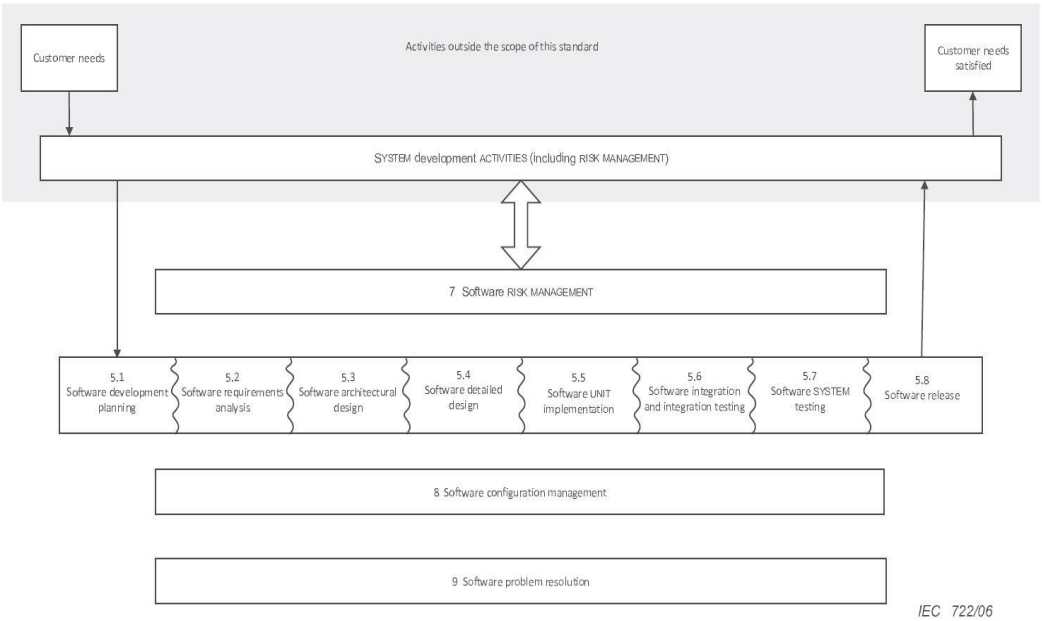


Figure 5: IEC 62304:2006/AMD 1:2015 Figure 1 – Overview of software development PROCESSES and ACTIVITIES[1]

The proposed process is considered to be an essential development process for medical device software and ensures, during the development process, that the necessary steps are planned, implemented and verified in a structured manner at an early stage.

According to IEC 62304, the development can, in principle, be implemented with agile development methods but, in practice, is associated with certain requirements that are difficult to satisfy with a purely agile process.

2.9.3 IEC 62366-1:2015/Amd1:2020 Application of usability engineering to medical devices

IEC 62366, usability

This standard concerns the usability of medical devices and the verification and validation thereof. IEC 62366 defines usability as the *characteristic of the user interface that establishes effectiveness, efficiency, ease of user learning and user satisfaction.* Under the MDD, manufacturers must ensure that their devices are as user-friendly as possible. They must thus minimise any risks and hazards that may arise from a lack of usability. In addition, prior knowledge and the user's technical knowledge and skills must be taken into account during development. This would exclude, for example, the use of a very small, barely legible font on a disposable syringe designed for older people. The standard also helps the app developer to keep the relevant user group in mind and become aware of potential hazards when a device is used by a specific group of patients.

2.9.4 ISO 14971:2019 Application of risk management to medical devices

ISO 14971, risk management

ISO 14971 is concerned with risk management in the development, manufacture and use of medical devices. Medical device manufacturers must prove that possible patient risks associated with their device are manageable. The standard thus calls for a risk analysis to be carried out for the device in question, and for the risks described to be reduced as far as possible. In addition, any residual risks must be additionally disclosed so that the risk-benefit ratio can subsequently be assessed in the clinical evaluation. Patient risks can arise, for example, from incorrect output (e.g. dose calculator) or a lack of output (e.g. reminder to take medication) due to software defects (bugs) or security vulnerabilities on mobile devices. Here, a

[1] IEC 62304 Ed. 1.1 Copyright © 2015 IEC Geneva, Switzerland. www.iec.ch

risk analysis must be used to estimate the risk of harm and the severity thereof. In a further step, measures must be defined to reduce this specific risk (cybersecurity, security updates, bug fixes...). In particular, it is important to bear in mind that a software update for an app which is a medical device is considerably more complex than for a "normal" app (verification, validation, documentation, information, etc.).

2.9.5 IEC 82304-1:2017 Health software - Part 1: General requirements for product safety

IEC 82304-1
health software

IEC 82304-1 was first published in 2016 with the aim of closing gaps in IEC 62304 with regard to the use of stand-alone software. IEC 82304-1 is applicable to all software products and apps which run on general computer systems, mobile phones or tablets and are intended to be used to maintain or improve the health of individuals or the delivery of care.

This standard is especially important for the validation of health software. It also plays a significant role for developers outside the medical device industry (e.g. developers of health/well-being/lifestyle apps).

2.9.6 IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle

IEC 81001-5-1

IEC 81001-5-1 supplements the software life cycle described in IEC 62304 concerning processes for guaranteeing IT security. The purpose of the standard is to increase the cybersecurity of health software by establishing certain activities and tasks in the software life cycle processes and also by increasing the security of software life cycle processes themselves.

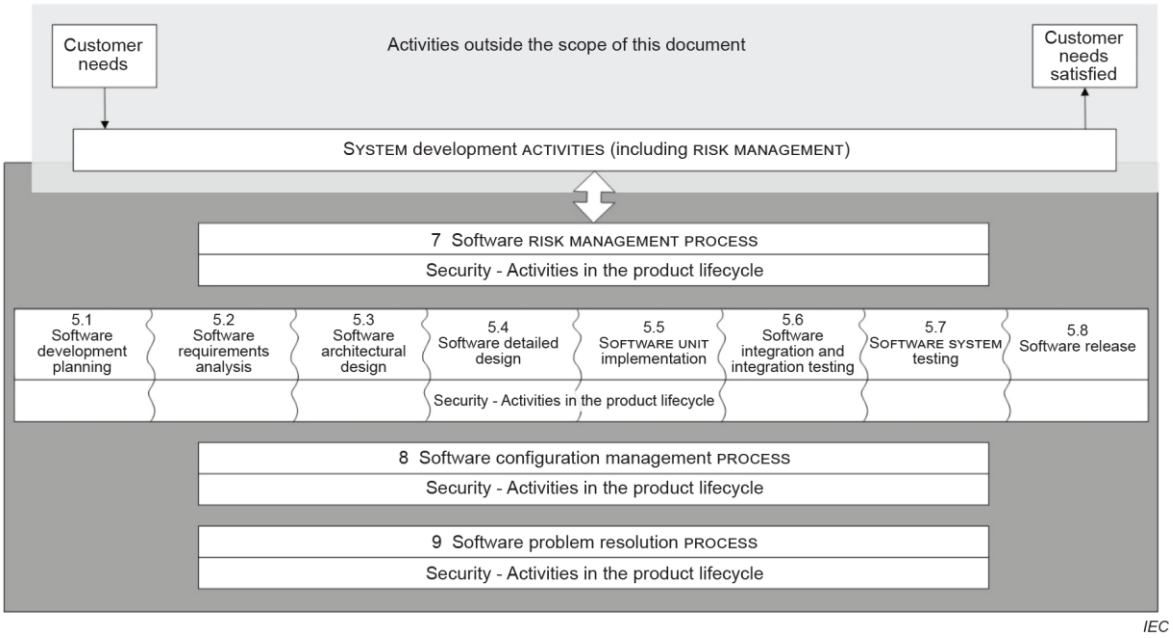


Figure 4: IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle (Figure 2)

Since the standard is to be harmonised to the MDR, it can be used to confirm compliance with the general safety and performance requirements.

2.9.7 IEC TR 60601-4-5:2021 Medical electrical equipment - Part 4-5: Guidance and interpretation - Safety-related technical security specifications

IEC TR 60601-4-5

The technical report IEC TR 60601-4-5 describes specific measures showing how IT security for medical devices can be managed at the technical level. In this context it refers to IEC 62443-4-2, which deals with IT security in industrial communication networks.

Security levels represent a key element of IEC TR 60601-4-5 and are used to describe the required security level of an IT network, as well as the security level implemented in a medical device or software. The security level defines what measures must be implemented and the scope of these measures. The aim is to ensure that the achieved security level (SL-A) after integration of the software is equivalent to, or higher than, the previously defined target security level (SL-T). A key factor to this end is the capability security level (SL-C) of the software, which is defined by the implementation of the technical measures described in the standard.

The technical report therefore serves as a guide to manufacturers of medical apps in fulfilling the corresponding general safety and performance requirements (GSPR) of MDR.

3 The Switzerland – EU situation

3.1 The key facts in brief

Under the old regulations (European MDD and old Swiss MedDO), and especially thanks to the Mutual Recognition Agreement (MRA), medical devices that were placed on the market in Switzerland could be marketed in Europe with no barriers, and vice versa. However, the MRA has not been updated in line with the new regulations (European MDR and new Swiss MedDO). Mutual recognition no longer applies, and Switzerland is now considered to be just a third country within the meaning of the MDR. Consequently, in order to access the EU market, Swiss manufacturers must designate an authorised representative domiciled in an EU member state (EU-Rep) and arrange for their devices to be placed on the market by an EU importer. Moreover, since Swissmedic does not have access to EUDAMED, the European database on medical devices, economic operators and devices must be registered with, and reports of incidents reported to, Swissmedic directly.

3.2 Switzerland as a third country within the meaning of the MDR

Mutual Recognition Agreement (MRA)

The Mutual Recognition Agreement (MRA) between Switzerland and EU regulates the mutual recognition of conformity assessment procedures and is an important instrument for reducing technical barriers in the marketing of numerous industrial products, including medical devices. The mutual recognition of the old European MDD and the Swiss MedDO was part of the MRA. These agreements simplified the reporting obligations of companies that placed devices on the market and allowed devices to be distributed directly from Switzerland to all EU and EFTA member states and to Turkey, without the need for an authorised representative domiciled in these countries. Conversely, companies domiciled in the contracting states could market medical devices directly in Switzerland.

By the date of application of the European MDR and the entry into force of the new Swiss MedDO on 26 May 2021, the MRA would have had to be updated in order to take account of the new regulations and maintain the free market access without additional requirements.

The EU had stipulated the conclusion of the Institutional Framework Agreement (InstA) with Switzerland as a precondition for drafting new, and updating existing, Bilateral Agreements. The discontinuation of the negotiations on InstA by the Federal Council on 26 May 2021 prompted the EU, in turn, to discontinue revisions of the MRA. Therefore, the mutual recognition of medical device regulations between Switzerland and the EU no longer applies.

Substantial parts of the Swiss MedDO refer directly to the MDR, and the requirements relating to the various economic operators and are largely identical with those of the MDR. Basically, the MedDO reads like the MDR, with adaptations of certain terms ('EU', 'Union' or 'member state' is replaced with 'Switzerland', 'third country' is referred to as 'abroad' or 'other country'). Thus, when the MDR refers, for example, to manufacturers from third countries, which means all non-EU/EEA countries and includes Switzerland, the MedDO refers to these as 'foreign manufacturers' which, in turn, also includes manufacturers from the EU. The aim of the revised MRA would have been largely to free economic operators in Europe and Switzerland of the obligations for foreign economic operators defined in the MedDO and MDR.

The fact that the MRA has not been updated in line with the new regulations has far-reaching consequences, particularly for Swiss manufacturers wanting to place their devices on the market in Europe.

3.3 EU authorised representative

EU authorised representative (EU-Rep)

Manufacturers from third countries, including Switzerland, must designate an authorised representative (EU-Rep) domiciled in an EU member state in order to place their devices on the market in the EU. On the one hand, the EU-Rep guarantees the existence of a legally actionable entity for the EU member states and, on the other, the EU-Rep itself is obliged to check the manufacturer's compliance with the regulations.

Manufacturers can designate any natural or legal person domiciled in the EU as their EU-Rep. This requires a written mandate, which must be signed by the manufacturer and the EU-Rep. The EU-Rep must have permanent and continuous access to a professional who is verifiably familiar with the regulatory requirements for medical devices in the EU (known as the “person responsible for regulatory compliance”, PRRC). Like the manufacturer, the EU-Rep must also be registered in EUDAMED (see section**Fehler! Verweisquelle konnte nicht gefunden werden.**) and obtain a Single Registration Number (SRN).

Tasks of the EU-Rep

The authorised representative becomes the primary contact person for the competent authorities in the EU and must fulfil the following obligations:

- Check compliance with the registration requirements
  The authorised representative must ensure that the manufacturer has produced an EU declaration of conformity and technical documentation for its devices. The authorised representative must also ensure that the devices have undergone a corresponding conformity assessment procedure. The authorised representative also checks whether manufacturers and importers have been correctly registered in EUDAMED and that the devices have received a correct UDI-DI and have been entered in EUDAMED.
- Keep documentation available
  The EU-Rep must keep available copies of the technical documentation, the EU declaration of conformity and, if applicable, copies of the certificates of conformity for the devices. The documents must be kept for up to 10 years after the devices were last placed on the market (15 years for implants). The documents must be presented to a competent authority on request.
- Assist the authorities during audits and product verifications
  Authorities can ask the EU-Rep to give them access to samples or test products. The EU-Rep must ensure that this access is also granted. The EU-Rep also assists the authorities with any preventive or correction actions relating to defective devices.
- Report incidents and complaints (Vigilance Report)
  The EU-Rep must inform the manufacturer immediately of incidents connected with devices for which it is responsible.

Joint liability of the EU-Rep

The EU-Rep is also legally liable, jointly and severally with the manufacturer, for defective devices if the manufacturer fails to fulfil its obligations defined in the MDR. It is therefore in the EU-Rep's own interests to carefully check the conformity of the devices and the manufacturer's compliance with the regulations. This extended liability also places stricter requirements on the EU-Rep's insurance cover.

For their part, manufacturers are obliged to make available to their EU-Rep all the required documents without any gaps, which also

includes, if necessary, confidential information in the technical documentation for the devices.

Product labelling

The EU-Rep must be stated on the product labelling (for software this can be done as for the rest of the 'label' e.g. on an easily accessible info screen). The following symbol, followed by the name and address, should preferably be used for this purpose:

Musterfirma
Lietzenburger Strasse 95
DE-84242 Tutzing

The information on the EU-Rep must also be stated on the declaration of conformity and on any certificate of conformity.

EU importer

In addition to the EU-Rep, manufacturers from third countries also need an importer to place their devices on the EU market. However, in contrast with the EU-Rep, importers are not designated by the manufacturer – basically any natural or legal person that places a device from a third country on the EU market becomes an importer within the meaning of the MDR. Nevertheless, the MDR requires close cooperation between manufacturers and importers, particularly as regards the processing of complaints and recalls.

3.4 Market surveillance in Switzerland

The status as a third country also has major implications for market surveillance in Switzerland. Along with the MDR, EUDAMED, the European database on medical devices, has also been introduced (see section **Fehler! Verweisquelle konnte nicht gefunden werden.**). EUDAMED primarily serves as a tool for the exchange of information between competent authorities in the EU member states, thereby facilitating the market surveillance and traceability of devices. Among others, economic operators (manufacturers, authorised representatives, importers and, if applicable, distributors) and devices are registered in EUDAMED.

The MedDO has largely been aligned with the MDR and accordingly stipulates the same requirements for the registration of economic operators and devices. But as a third country, Switzerland and its competent authority Swissmedic, now has no access to EUDAMED, and the direct exchange of information between Swissmedic and the competent authorities of the EU member states no longer takes place. Therefore, in order to guarantee a functional market surveillance system within Switzerland, manufacturers, authorised

representatives and importers must register with Swissmedic and request a "Swiss Single Registration Number", or CHRN, similar to the SRN in Europe. In future, devices will also need to be registered via Swissmedic. When this will be necessary and the detailed procedure for device registration have not yet been established. An electronic system for Switzerland similar to EUDAMED is currently being set up, but the exact modalities are not yet known.

Manufacturers that place their devices on the market in Switzerland and the EU must therefore register themselves and their devices both with Swissmedic and in EUDAMED. Reportable incidents with devices must also be reported to Swissmedic and, if necessary, in EUDAMED (see section **Fehler! Verweisquelle konnte nicht gefunden werden.**).

4 Medical software under the MedDO and MDR

4.1 The key facts in brief

The transitional period for the new European Medical Device Regulation (MDR) ended on 26 May 2021. At the same time the new MedDO entered into force in Switzerland. The MDR and new MedDO have introduced a number of significant changes, which also need to be taken into account particularly by manufacturers of medical software (medical device software, MDSW). These include a stricter classification rule for medical software, increased requirements for clinical evaluations, post-market surveillance and vigilance, and the introduction of EUDAMED, the database on medical devices.

4.2 Qualification and classification

While the basic definition which determines whether or not software is a medical device has largely remained the same, the MDR has brought significant changes to the risk classification of medical software. A large proportion of the software that was classified as Class I under the Medical Device Directive (MDD) is assigned to a higher class under the MDR, which has a considerable impact on the effort which manufacturers have to invest in certification.
The changes in classification are a result of Rule 11 in Annex VIII to the MDR (Classification Rules).

4.2.1 Classification according to Rule 11

In the MDD, medical software was classified according to the classification rules for active medical devices. However, these rules are not specifically designed for software, but rather for active devices which deliver energy or substances to, or remove them from,

Regulation (EU) 2017/745, Annex VIII

the body. The risk which may arise for the patient as a result of incorrect information provided by software is not addressed.

For this purpose, Rule 11 was included in the MDR. This states that:

Classification Rule 11

Software intended to provide information which is used to take decisions for diagnostic or therapeutic purposes is classified as class IIa, except if such decisions have an impact that may cause:

- *death or an irreversible deterioration of a person's state of health, in which case it is in Class III; or*
- *a serious deterioration of a person's state of health or a surgical intervention, in which case it is classified as Class IIb.*

Software intended to monitor physiological processes is classified as class IIa, except if it is intended for monitoring vital physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient, in which case it is classified as class IIb.

All other software is classified as Class I.

4.2.2 EU Guidance – MDCG 2019-11

In October 2019, guidance on the qualification and classification of medical device software (MDSW) under the MDR and IVDR was issued by the EU Medical Device Coordination Group (MDCG). Although this document is not legally binding, it does have considerable weight.

MDCG 2019-11

The guidance provides assistance with the qualification of software as a medical device and the classification thereof. This includes a different presentation of Rule 11, which does not however necessarily lead to a better understanding of this rule, which is already clearly defined.

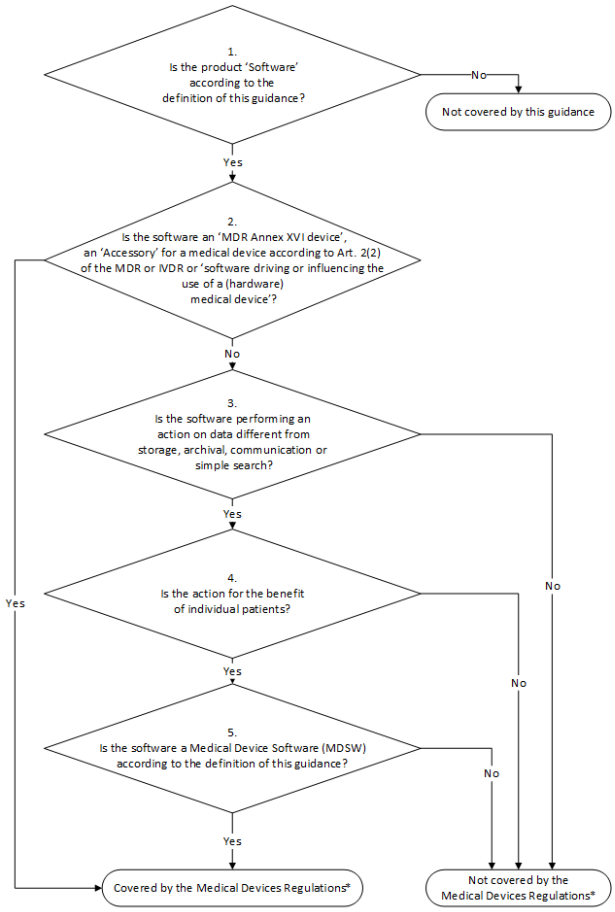
Assistance and decision diagrams

In the guidance, Rule 11 is divided into three sub-rules, which are applied depending on the intended use/purpose of the MDSW:

- 11a) (first three paragraphs of Rule 11) intended to provide information which is used to take decisions with diagnostic or therapeutic purposes (class IIa–III);
- 11b) (Paragraph 4 of Rule 11) intended to monitor physiological processes or parameters (class IIa, IIb);
- 11c) (Paragraph 5 of Rule 11) all other uses (class I).

A decision diagram and the associated questions serve as a guide to the qualification of software as a medical device.

Figure 7: Decision steps to assist qualification of MDSW (source: MDCG 2019-11 Guidance).



A further decision diagram provides assistance in assessing whether medical software is to be qualified as medical device software (covered by the MDR) or as in vitro diagnostic medical device software (covered by the IVDR).

In addition, a table illustrates the relationship between the MDR risk classes and the framework for software risk categorisation of the International Medical Device Regulators Forum (IMDRF). Here, risk categories are based on the combination of the significance of the information provided by the software to a healthcare decision and the healthcare situation or patient condition.

State of Healthcare situation or patient condition		Significance of Information provided by the MDSW to a healthcare situation related to diagnosis/therapy		
		High Treat or diagnose *~ IMDRF 5.1.1*	**Medium** Drives clinical management *~ IMDRF 5.1.2*	**Low** Informs clinical management *(everything else)*
	Critical situation or patient condition *~ IMDRF 5.2.1*	**Class III** *Category IV.i*	**Class IIb** *Category III.i*	**Class IIa** *Category II.i*
	Serious situation or patient condition *~ IMDRF 5.2.2*	**Class IIb** *Category III.ii*	**Class IIa** *Category II.ii*	**Class IIa** *Category I.ii*
	Non-serious situation or patient condition *(everything else)*	**Class IIa** *Category II.iii*	**Class IIa** *Category I.iii*	**Class IIa** *Category I.i*

Figure 8: Illustration of the relationship between the MDR risk classes and IMDRF risk categories (source: MDCG 2019-11 Guidance).

Finally, the guidance provides a number of examples illustrating the rules for qualification as a medical device and for classification.

It is clear from the guidance that the MDCG interprets Rule 11 rather strictly. Firstly, the provision of iinformation used to take decisions with diagnostic or therapeutic purposes is stated to be characteristic of all MDSW, and sub-rule 11a) – making no provision for classification as Class I – is therefore generally applicable to all MDSW. Secondly, the risk categories I and II defined in the IMDRF document both correspond to MDR risk class IIa. This once again makes it clear that, under the MDR, most medical software can no longer be classified as Class I. The only example of Class I software mentioned in the MDCG document is an app intended to support conception by calculating the user's fertility status.

4.2.3 Implications for manufacturers of MDSW

For medical devices classified as higher than Class I, manufacturers must involve a notified body in the conformity assessment. This means that the compliance of the software with the requirements of the MDR can not be declared by manufacturers themselves, on their own responsibility, but has to be assessed and certified by a notified body.

In most cases, this means that a complete quality management system (QMS) in accordance with ISO 13485 must also be established and certified. Particularly for smaller companies and start-ups, the establishment of a QMS involves massive additional investments of time and financial resources.

Devices that were Class I devices under the MDD, and which are to be assigned to a higher risk class in accordance with the classification rules of the MDR – as is frequently the case for medical software – may continue to be placed on the market until 26 May 2024, provided that the declaration of conformity under the MDD was drawn up prior to 26 May 2021, and there are no significant changes in the design or intended purpose of the devices. In addition, the requirements of the MDR concerning post-market surveillance and vigilance must be complied with.

Transitional period

4.3 European database on medical devices (EUDAMED)

The MDR has resulted in the launch of the database on medical devices EUDAMED. The purpose of this database is to centralise all the relevant information on economic operators and devices, and to ensure traceability. In particular, the objectives of EUDAMED are as follows:

- enhancing transparency, by providing users with adequate access to information on devices and the relevant economic operators
- improving market surveillance (e.g. through unambiguous identification of devices and facilitated traceability)
- avoiding multiple reporting requirements
- enhancing coordination between member states
- streamlining the flow of information between economic operators, notified bodies or sponsors and member states and the Commission

EUDAMED consists of a number of modules:

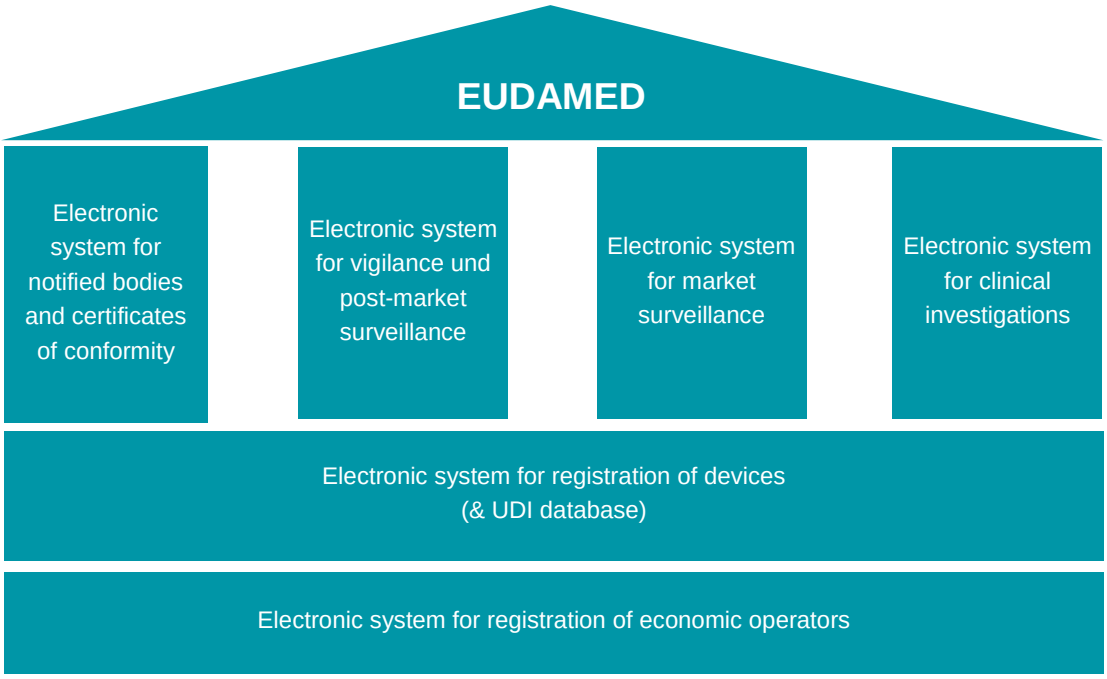


Figure 9: Modules of EUDAMED (graphic: ISS AG).

EUDAMED modules

Registration of economic operators

Manufacturers, importers and authorised representatives must register in EUDAMED. After registration, the economic operator is issued with a single registration number (SRN), permitting unambiguous identification.

Registration of devices/UDI

This module will contain all device-specific information associated with the UDI system. The UDI system consists of the Basic UDI-DI, which identifies a device model (group of devices with similar properties), and the UDI-DI, which identifies a specific model of a device. A Basic UDI-DI can thus cover a number of different UDI-DIs, whereas a UDI-DI is linked to a single Basic UDI-DI.

Notified bodies and certificates of conformity

This module will be used to manage information on notified bodies and the status of conformity assessment procedures. In addition, certificates of conformity (CE certificates) issued by notified bodies will be stored here.

Vigilance and post-market surveillance

Serious incidents and safety corrective actions will be documented in this module. Also to be stored here are manufacturers' periodic

summary reports and trend reports, as well as periodic safety update reports and safety notices. This system will be directly linked to the UDI database.

Market surveillance
This module will primarily be used by the member states' competent authorities to exchange information on market surveillance.

Clinical investigations
All clinical investigations must also be registered in EUDAMED. Clinical investigations can thus be clearly identified and monitored.

Data entry and date of introduction

Data is either to be entered in online forms or submitted via a user interface (XML).

The modules *Registration of economic operators*, Registration of devices/*UDI* and *Notified bodies and certificates of conformity* are currently available. The other three modules are scheduled to go live at the end of 2023.

Corresponding system for Switzerland

Since Switzerland is now considered to be a third country within the meaning of the MDR (see section **Fehler! Verweisquelle konnte nicht gefunden werden.**) Swissmedic does not have access to EUDAMED. However, the MedDO stipulates the same registration and reporting requirements as the MDR. A corresponding system for Switzerland is currently being developed at Swissmedic. The Swiss medical devices database will be similar to the European EUDAMED, but the precise modalities are not yet known.

4.4 Clinical evaluation

Manufacturers of medical devices are required to produce a clinical evaluation report (CER) for all their devices – irrespective of the risk classification. The main objective of this process is to demonstrate the safety, the performance and the clinical benefits of medical devices. This generally requires data from the clinical application of the medical device; the requirements concerning the quantity and quality of such data largely depend on the risk classification.

Clinical evaluation is an integral part of the quality management system and the technical documentation of medical devices. It serves, for example, as a basis for risk management, justifying the

assumptions made concerning benefits and the acceptability of the benefit-risk ratio.
A clinical evaluation is initially conducted as part of the conformity assessment procedure, with the report being regularly updated after the device has been placed on the market.

4.4.1 Regulatory basis and guidance

The objectives of a clinical evaluation are defined in Article 61 of the MDR, and the procedure is set out in Annex XIV. The clinical evaluation should demonstrate, on the basis of clinical data, that a device fulfils the applicable general safety and performance requirements specified in Annex I to the MDR.

In general, the same requirements are applicable to the clinical evaluation of medical software as for any other medical device. In addition, the International Medical Device Regulators Forum (IMDRF) has issued a guidance document (IMDRF/SaMD WG/N41), specifically addressing the clinical evaluation of software as a medical device. In March 2020, the Medical Device Coordination Group published Guidance on Clinical Evaluation (MDR)/Performance Evaluation (IVDR) of Medical Device Software - MDCG 2020-1, which also makes reference to the IMDRF document.

4.4.2 Clinical data

Clinical data

“Clinical evaluation” is defined as a systematic and planned process to continuously generate, collect, analyse and assess the clinical data pertaining to a device.

“Clinical data” is defined as information concerning safety or performance that is generated from the use of a device and is sourced from the following:

- clinical investigation(s) of the device concerned,
- clinical investigation(s) or other studies reported in scientific literature, of a device for which equivalence to the device in question can be demonstrated,
- reports published in peer-reviewed scientific literature on other clinical experience of either the device in question or a device for which equivalence to the device in question can be demonstrated,
- clinically relevant information coming from post-market surveillance, in particular the post-market clinical follow-up.

Clinical data can thus be collected in various ways – through clinical studies of the device in question or an equivalent device, from scientific reports on such devices, from information in product safety databases, or through post-market surveillance/vigilance. For Class III and implantable devices, a clinical study of the device in question is essential in most cases. For all devices in lower risk classes, the clinical evaluation may be based on data obtained from clinical experience with equivalent devices.

For a device to be deemed equivalent, it must share certain characteristics with the manufacturer's own device. In the case of software, this involves technical aspects such as similar conditions of use, specifications and properties (software algorithms), and similar deployment methods, principles of operation and critical performance requirements. In addition, the devices must be used for the same clinical condition or purpose (e.g. in the same disease, in a similar population), have the same kind of user, and have similar relevant critical performance.

4.4.3 Clinical evaluation of software

Requirements for clinical evaluation

Stand-alone software differs from classical medical devices in several respects, which also has implications for the clinical evaluation.

In the IMDRF document "Software as a Medical Device (SaMD): Clinical Evaluation" (IMDRF/SaMD WG/N41), the clinical evaluation of medical software is defined as "the assessment and analysis of clinical data pertaining to a medical device to verify the clinical safety, performance and effectiveness of the device when used as intended by the manufacturer. It is based on the following three principles:

- Valid clinical association: Is there a valid clinical association between the SaMD output and the SaMD's targeted clinical condition?
- Analytical/technical validation: Does the SaMD correctly process input data to generate accurate, reliable, and precise output data?
- Clinical validation: Does use of the SaMD's accurate, reliable, and precise output data achieve the intended purpose in the target population in the context of clinical care?

A valid clinical association can in principle be demonstrated by a review of the clinical literature. The aim is to show the extent to which the SaMD's output (concept, conclusion, measurements) is clinically accepted or well-founded and corresponds accurately to the target healthcare situation or clinical condition.

The aim of the analytical/technical validation is to confirm that the software was correctly constructed – namely, that it correctly and reliably processes input data and generates output data with the appropriate level of accuracy, and repeatability and reproducibility (i.e. precision). It also demonstrates that the software meets its specifications, and that these specifications conform to user needs and intended uses. This information is usually generated during the verification and validation phase of the software development life cycle.

Clinical validation, lastly, measures the ability of a SaMD to yield a clinically meaningful output in the target health care situation. Here, clinically meaningful means the positive impact of a SaMD on the health of an individual or population, to be specified as measurable, patient-relevant clinical outcome(s), including outcome(s) related to the function of the SaMD (e.g. diagnosis, treatment, prediction of risk, prediction of treatment response).
Clinical validation of a SaMD can also be viewed as the relationship between the verification and validation results of the SaMD algorithm and the clinical conditions of interest.
According to the IMDRF document, clinical validation can be demonstrated in various ways:

- by referencing existing data from studies conducted for the same intended use;
- by referencing existing data from studies conducted for a different intended use, where extrapolation of such data can be justified; or
- by generating new clinical data for a specific intended use.

Here it should be noted that, given the more stringent requirements in the MDR concerning device equivalence, it will be difficult to show clinical validation on the basis of data from studies of other devices.

4.5 Post-market surveillance and vigilance

PMS and vigilance

The MDR places particular emphasis on the collection of clinical and safety-related data (post-market surveillance/PMS) following CE certification (self-declaration for Class I) and market access. Monitoring of the performance of CE-labelled devices is crucial to permit systematic identification of risks associated with the use of the medical device in practice (and thus also previously unknown risks) and ongoing demonstration of its benefits. Only through continuous and systematic surveillance can manufacturers ensure that their medical devices are safe, and that there are no uncontrolled risks.

4.5.1 Regulatory basis

PMS requirements

In Article 83 of the MDR, post-market surveillance is defined as a system established by manufacturers (in cooperation with other economic operators) for proactively and systematically collecting information on experience with, and the performance of, medical devices, so as to identify any need for preventive or corrective actions (CAPA).

The requirements for post-market surveillance also involve a risk-based approach, as the system adopted is to be proportionate to the risk class and appropriate for the type of device. Although surveillance activities are required for all medical devices, irrespective of risk class, the nature of the requirements varies.

Analysis of the data gathered by the post-market surveillance system may lead to the technical documentation being updated; in particular, this data is to be used:

- to update the benefit-risk determination;
- to improve risk management;
- to update the design and manufacturing information, the instructions for use and the labelling;
- to update the clinical evaluation (see Section **Fehler! Verweisquelle konnte nicht gefunden werden.**);
- to update the summary of safety and clinical performance (only applicable for Class III and implantable devices);
- for the identification of needs for preventive, corrective or field safety corrective action; and
- to detect and report trends.

The manufacturer's post-market surveillance system must be based on a post-market surveillance plan (Article 84), which is to be part of the technical documentation, serving to prove the manufacturer's compliance with the relevant PMS requirements. Annex III specifies the requirements and content of a post-market surveillance plan, which must address the collection and utilisation of available information and cover, at least, the following:

- a proactive and systematic process to collect any relevant available information. The process shall allow a correct characterisation of the performance of the devices and shall also allow a comparison to be made between the device and similar products available on the market;
- effective and appropriate methods and processes to assess the collected data;
- suitable indicators and threshold values that shall be used in the continuous reassessment of the benefit-risk analysis and of risk management;
- effective and appropriate methods and tools to investigate complaints and analyse market-related experience collected in the field;
- methods and protocols to manage the events subject to the trend report as provided for in Article 88, including the methods and protocols to be used to establish any statistically significant increase in the frequency or severity of incidents as well as the observation period;
- methods and protocols to communicate effectively with competent authorities, notified bodies, economic operators and users;
- reference to procedures to fulfil the manufacturer's obligations relating to post-market surveillance;
- systematic procedures to identify and initiate appropriate measures including corrective actions;
- effective tools to trace and identify devices for which corrective actions might be necessary; and

- a post-market clinical follow-up (PMCF) plan as referred to in Part B of Annex XIV, or a justification as to why a PMCF is not applicable.

Annex III also specifies the types of available information that must be proactively and systematically collected and utilised for post-market surveillance:

- information concerning serious incidents, including information from periodic safety update reports, and field safety corrective actions;
- records referring to non-serious incidents and data on any undesirable side-effects;
- information from trend reporting;
- relevant specialist or technical literature, databases and/or registers;
- information, including feedbacks and complaints, provided by users, distributors and importers; and
- publicly available information about similar medical devices.

4.5.2 Post-market surveillance report

Surveillance report

Manufacturers of Class I devices are required to prepare a post-market surveillance report summarising the results and conclusions of the analyses of the data gathered as a result of the post-market surveillance plan (Article 85). The report must include a rationale and description of any preventive and corrective actions taken, and is to be updated when necessary.

4.5.3 Periodic safety update report

Periodic safety update report (PSUR)

Manufacturers of Class IIa, Class IIb and Class III devices are required, throughout the lifetime of each device, to prepare a periodic safety update report (PSUR) (Article 86). This report summarises the results and conclusions of the analyses of the post-market surveillance data, including, in particular, the conclusions of the benefit-risk determination, a rationale and description of any preventive and corrective actions taken, the main

findings of the post-market clinical follow-up, the volume of sales of the device, and information on the population using the device.
The safety update report, which is part of the technical documentation, must be updated at least every two years for Class IIa devices and at least annually for Class IIb and III devices.
Manufacturers must make PSURs for Class IIa and IIb devices available to the notified body and, on request, to competent authorities.
PSURs for Class III devices must be submitted to the notified body via EUDAMED (as soon as the database has been introduced).
The notified body will review the report and add its evaluation, and the two documents are subsequently to be made available (again through EUDAMED) to competent authorities. A PSUR may cover a number of medical devices. PSUR guidance and a template are currently being prepared at the European level.

4.5.4 Requirements for post-market clinical follow-up (PMCF)

Under Part B of Annex XIV, manufacturers are required to conduct a post-market clinical follow-up (PMCF), proactively collecting clinical data so as to answer important questions on the safety and performance of the device, and to update the clinical evaluation.

PMCF

Post-market surveillance data and information must be included in the post-market section of the clinical evaluation report.

Manufacturers must conduct the PMCF process in accordance with a PMCF plan and document the results in a PMCF evaluation report that is to be part of the clinical evaluation report and the technical documentation. The conclusions of the PMCF evaluation report may also lead to an update of the risk management documents.

4.5.5 Vigilance

Vigilance, which is part of post-market surveillance, refers to the system whereby manufacturers are required to report serious incidents and field safety corrective actions (FSCAs) to the competent authorities; it also covers the requirements for recalls. Article 87 of the MDR defines the incidents which are to be reported and how such reports are to be submitted. Article 89 specifies the requirements for manufacturers' analysis of vigilance data.

Vigilance

Manufacturers are required to report immediately any serious incident or any field safety corrective action in respect of devices. Since January 2020, manufacturers have been required to use a reporting template – the Manufacturer Incident Report (MIR). The reporting periods specified for manufacturers in the MDR vary according to the type of incident:

- serious incident: immediately, not later than 15 days after they become aware of the incident
- serious public health threat: immediately, not later than 2 days after they become aware of the threat
- death or unanticipated serious deterioration in a person's state of health: immediately, not later than 10 days after they become aware of the incident.

In addition, all serious incidents must be investigated by the manufacturer; the investigations must include a risk assessment of the incident and field safety corrective action. The manufacturer must ensure that information about the field safety corrective action taken is brought without delay to the attention of users of the device in question (via EUDAMED, as soon as the database is operational).

In consultation with the competent authorities, manufacturers may provide periodic summary reports (instead of individual serious incident reports) for similar serious incidents that occur with the same device or device type, provided that the root cause has been identified or a field safety corrective action implemented, or where the incidents are common and well documented. The authorities and manufacturer must also have agreed on the format, content and frequency of the periodic summary reporting.

Article 88 of the MDR also regulates trend reporting, with manufacturers being required to report any statistically significant increase in the frequency or severity of incidents that are not serious incidents or that are expected undesirable side-effects. Such trends could have an impact on the benefit-risk analysis and could involve unacceptable risks. In the post-market surveillance plan, the manufacturer specifies the observation period and the methodology used for determining any statistically significant increase in the frequency or severity of such incidents.

5 Is agile development possible for MedTech?

5.1 Brief summary of the key points

Agile development is also possible for MedTech applications. However, certain compromises are required. The relevant standard lists some points that must be taken into account. The essential compromise is that the relevant documentation must be completed and released at defined milestones.

5.2 Agile development process

Agile development despite IEC 62304

Today, most software is developed in an iterative process. The fairly rigid and sequential V-model from IEC 62304 conflicts with agile methods to a certain extent.

V-model

The V-model requires a sequential development process:

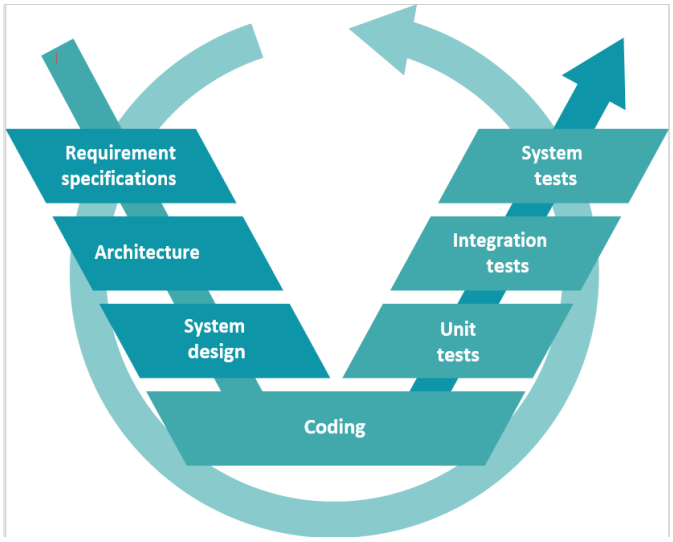


Figure 10: Simplified V-model (graphic: ISS AG)

However, this conflict can be resolved. The following points are relevant:

- Interpret the V-model as a document landscape and not as a rigid development process.
- Create and release a software development plan (especially a document plan) at the start of the project.
    - Continuously adapt the draft of the plan during the project (but do not release it with every change).
    - Release the plan only in case of significant changes.
- Successively adapt all documents; the requirements and design must be released at the latest prior to test activities (verification).
- Plan reviews and regularly conduct and document them.

- Prepare and check for a complete and consistent documentation status for a release (reviews); see also the corresponding checklist.

5.3 Standards-based embedding

There are no standards governing agile programming for use in medical technology. However, there is a highly regarded Technical Information Report from the Association for the Advancement of Medical Instrumentation (AAMI). We recommend adhering to the recommendations given in TIR45 when defining your own process for software development using agile methods. The complete report must be purchased.

Technical Information Report

5.3.1 Tool validation

IEC 62304 also requires validation of the tools used for development. Here too, a technical report is available from the AAMI (TIR 36). In order to validate the development toolchain, it is recommended to comply with this report. The complete report must be purchased.

Validation of development tools

6 Cybersecurity

6.1 Brief summary of the key points

Manufacturers are obliged to consider software-specific hazards and risks, to identify them in the risk analysis and to take appropriate measures to reduce the risks. As a prerequisite for an adequate security concept, the initial security considerations and requirements must be defined already during the design stage. How to go about testing the potential hazards and risks is not regulated; this must be adapted to suit the particular software and its functions. In order to counteract risks that are not yet known at the time of development, an ongoing process is required. The manufacturer's obligations also include introduction of a product surveillance system and incorporation of the knowledge gained in this manner into the manufacture and further development of the product.

Cybersecurity & security requirements for medical devices

Due to the risk-based development approach specified for medical devices by the MDR and MedDO, an appropriate safety/security concept is required for every medical device, and software is no exception. Indeed, since it can be assumed that a network-enabled device will come into contact with malware, it must be ensured that no patient or operator risk arises. Here, software-specific hazards and risks must be taken into account; manufacturers of medical software are obliged to keep patient risks as low as possible and take appropriate measures. The MDR generally represents a tightening of the regulation of medical devices (with the aim of protecting patients). Medical software, in particular, is usually classified in one of the higher risk classes as a result of the new classification rule 11. Higher risk classes imply more stringent regulatory requirements, also with regard to security and the verification of security. When software is certified in or as a medical device, it is necessary to document and prove that adequate security measures have been implemented and that performance and the protection of sensitive data are assured.

Developers need to define the initial security considerations and requirements starting in the design stage. There are multiple reference points in the development process for ensuring and testing security:

- During the definition of the device requirements
- During the development of the device architecture
- During the preparation of the risk analysis
- During verification and validation
- During product maintenance/sustaining engineering (updates, bug fixes, etc.)

Security begins with design

Nowadays, medical software is used to perform a diverse range of functions in or as a medical device, e.g. control of complex medical equipment as well as processing and storage of data. Given the diversity of the functions, the risks (and vulnerabilities) are also numerous – as are the consequences of potential malfunctions in programmable medical devices. Networked medical devices in particular are susceptible to manipulation and unauthorised access, and data protection must be assured. This can be achieved only if these points are taken into account beginning with the conception and **design of the software**. The earlier in the process that risk management is implemented, the simpler and more sustainable the security concept. Typical points are e.g.

- Interconnection with networks/other devices (connectivity)
- Access protection and permissions
- Logins (password policies, removal of old accounts, etc.)
- Automatic logoff from application
- Network communication and server security
- Access protection for backups
- Data encryption (Must the data be encrypted? If so, how? And how should communication with less secure encryption standards be managed?)
- Data archival and deletion
- Data integrity
- Software updates

Risk analysis

Various factors are relevant in determining the measures to be taken; thus, as well as specifying a security concept, all foreseeable risks must be minimised (or eliminated). Special attention must be paid to specific patient and operator risks. These risks must be identified and analysed in the context of measures that are technically feasible and appropriate for the risks. The risk management standard ISO 14971 (see Section 2.9.4) provides guidance on evaluating risks in relation to the use environment and intended purpose. For software, preparation of a risk management analysis is an important step towards meeting security requirements. The risks are not only analysed but also documented, and relevant measures are evaluated and defined in relation to their effectiveness for risk control. The state of the art is a decisive factor in determining which measures are technically feasible; in many cases, this is also decided on the basis of expert knowledge and is not necessarily defined in standards. Compliance with IEC 62304 (see Section

2.9.2), which is relevant for the development of software, as well as IEC 82304 (see Section 2.9.5), is mandatory. IEC 62304 is currently undergoing revision. In the current draft, requirements for security measures have been explicitly formulated for the first time.

Verification and validation

How to go about testing the potential hazards and risks is not strictly regulated; this must be adapted to the particular software and its functions. The following steps are often taken to evaluate security:

- Testing of security protocols
- Fuzz testing
- Software testing using targeted attacks by experts

Security after market launch

Despite all possible measures, 100% security cannot be achieved. Since manufacturers continue to have obligations after software has been developed, they must provide appropriate processes for secure updates and be able to respond to any security risks that arise. It is thus crucial to identify and be aware of all potential risks, as far as possible, during the manufacturing process. Since new risks can also arise that are not yet known at the time of development, an ongoing process is required. Manufacturers' obligations also include the introduction of a product surveillance system and incorporation of the knowledge thus gained into product manufacture and further development.

Legal foundations

There are no specific legal requirements in the EU concerning cybersecurity for medical devices. However, the requirements are implicit in the risk-based development approach specified in the regulations, as an appropriate security concept is mandated. As soon as a notified body becomes involved, it will assess whether the measures taken are appropriate and sufficient. The MDR also references IEC 62304. Although it only touches on cybersecurity, it does explicitly address this topic. In addition, the standards IEC 81001-5-1 and IEC TR 60601-4-5 will be harmonised with the MDR. Both standards address the cybersecurity of medical devices in networks (see Sections 2.9.6 and 2.9.7).

The FDA has published a number of guidance documents on cybersecurity. These documents are not legally binding, but they may be helpful during development. Guidance of interest includes the following:

Guidance	Comments
Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Recommends making cybersecurity part of software validation and the software risk process. Defines consensus standards from other areas that can be applied.
Postmarket Management of Cybersecurity in Medical Devices	Cybersecurity is part of the risk process and post-market management.
Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	FDA recommendations and position on the topic of cybersecurity/security updates for off-the-shelf software in devices; responsibilities, validation, etc.

Developments and guidance in other countries:

The fact that the topic of cybersecurity and data protection for medical devices has yet to be fully clarified is also shown by the many efforts being undertaken by national governments to regulate this area and make expert knowledge available.

In June 2017, for example, Ireland's Health Products Regulatory Authority published a Guide To Placing Medical Device Standalone Software on the Market. In July 2019, Australia's Therapeutic Goods Administration issued Medical device cyber security guidance for industry, dealing with cybersecurity and data protection.

In January 2020, the EU Medical Device Coordination Group (MDCG) published Guidance on Cybersecurity for medical devices (MDCG 2019-16). This document aims to provide manufacturers with guidance on how to fulfil the requirements of Annex I to the MDR and IVDR with regard to cybersecurity. It explains, for example, which requirements of these Regulations are relevant to cybersecurity and refers to other relevant regulatory documents (e.g. the IMDRF guidance).

Typical security considerations when reviewing software:

Review topic	Description
SOUP	Does the software or system contain software of unknown provenance (SOUP)? Identification of SOUP and software versions used

Fixed passwords or keys	Does the software use fixed passwords or keys that are the same on all devices or installations?
Human interface user input	Is the user input validated and restricted to valid ranges? Are the valid ranges defined? Has this been tested?
Machine interface network	Is the communication protected against deliberate or accidental manipulation?
Machine interface file formats	Are the data formats clearly defined? Is the data protected against changes?

Threat model

The threat model represents a potential approach for dealing with security requirements for medical software. This model defines potential objects to be protected by suitable measures, as well as potential attackers, patient or operator risks, and attack vectors.
The following tables represent a typical (but incomplete) threat model:

Protected objects

The first step is to list the objects or processes to be protected

Protected object	**Comments**
Patient data	Relevant for software that processes/analyses/stores patient data
Business data	Relevant for software that processes/analyses/stores business data
Device/system integrity	DoS/ransomware/extortion
Device/system operation	DoS/ransomware/extortion

Attackers

Potential attackers are identified and their motivation and the respective likelihood of an attack are defined.

Attackers	**Motivation**	**Probability**
Activist	Ideological	To be defined
Hacker	Recreational	To be defined
Hacker	Commercial	To be defined
Competitor	Commercial	To be defined
Criminal	Commercial	To be defined
...		

Attack vectors

Finally, possible attack vectors are described, i.e. ways and means whereby an attacker might gain access to a system.

Vector	**Description**
Physical device interface	USB, serial, network
Logical device interface	Human interface, machine interface
...	

Security concepts

There are also various security concepts and principles that can be used to fulfil the security requirements applicable to software:

Concept/principle	**Description**
Defence in depth	Security measures are implemented not only at the boundaries of the system but also within the system.
Least privilege	A process or software component should only have as many rights and privileges as are needed to perform the defined task.
Minimisation	Only software and services that are required should run on a device; this leads to a reduction in the attack surface.
Compartmentalisation	Different services/software/applications run in isolation from one other and only communicate via defined interfaces. Devices do not have any information that can be used directly to attack other devices (e.g. fixed passwords or keys).
Audit trail	Activities are logged

Adapted from Fundamental Security Concepts

These concepts also serve as a basis for guaranteeing data security in connection with data protection and corresponding requirements arising from the Swiss Data Protection Act.

7 Legal basis for data protection and security in Switzerland

7.1 Brief summary of the key points

From the perspective of data protection legislation, the requirements applicable to data processing in the area of health apps are strict or very strict, as the data in question is sensitive personal data. Manufacturers are obliged to comply with the legal requirements and to ensure risk-appropriate data security through technical and organisational measures. Whenever personal data from the EU is processed, the stricter EU requirements must also be observed.

7.2 Applicability of data protection legislation

Legislation and scope

Data protection legislation consists of the Data Protection Act and the Data Protection Ordinance. This legislation is derived from the fundamental right to informational self-determination. It is applicable whenever **"processing (a) of personal data (b)"** occurs:

(a) The term **"processing"** encompasses practically any operation involving personal data – e.g. the collection, storage, use, revision, disclosure (making accessible), archiving or destruction of data. It is irrelevant whether the data is processed electronically or in paper form. In the event of electronic processing, the means or services used for processing are also irrelevant. Many types of electronic processing involve profiling activities. Profiling is defined as the use of automated processing of personal data to evaluate certain aspects of a person. The objective of profiling activities is, for example, to analyse or predict a person's health, performance at work or economic situation. Profiling activities are also covered by the term "processing".

(b) "Personal data" means any information relating to an identified or identifiable person. Persons are identifiable if they can be identified by reference to an identifier, such as a name or number. Data protection legislation distinguishes between two types of personal data:

- **Normal personal data** – e.g. name, address, date of birth

- **Sensitive personal data** – e.g. health data, genetic or biometric data, data on religious, ideological or political views, data on social security measures

Processing of sensitive personal data and profiling activities are subject to more stringent requirements than processing of normal personal data.

Data protection in the area of medical apps

In connection with health apps, sensitive personal data is processed in the form of health data and also, in some cases, genetic or biometric data. In addition, processing often includes profiling activities. Accordingly, from the perspective of data protection legislation, strict or very strict requirements are applicable to the processing of personal data in the area of health apps.

Sensitive personal data

Data protection legislation contains a number of requirements that must be observed in the processing of sensitive personal data and profiling activities. The most important requirements are explained below:

Consent or legal basis

Processing of personal data requires either the consent of the data subject or a legal basis that allows the relevant data processing. If the data processing is based on consent, the consent is valid only if it meets the following conditions: It is given for a specific processing purpose or purposes, following the provision of adequate information, and is voluntary, unequivocal and explicit.

Since data processing in the context of health apps is generally based on the user's consent, such consent must be obtained. In order for the consent to be valid, users must consent to one or more specific processing purposes. In addition, the consent must be voluntary (given without pressure), unequivocal (not subject to doubt) and explicit (ideally in writing and thus verifiable).

Purpose limitation

When the data is collected, the purposes for which it is collected must be clear to the data subjects. A subsequent change of purpose is only permissible with the consent of the data subjects.

If the app provider specifies use of the app as the purpose of data processing, the data collected may not be used for advertising purposes or be transferred to third parties – unless the users consent to the use of their data for these further purposes.

Data minimisation (proportionality)

Only as much data may be collected and processed as is necessary to achieve the stated purpose of data collection. If the data processor wishes to collect or process more data, it may do so only if the data subjects have consented to such further data collection or processing. Data which is no longer required must be deleted or anonymised by the data processor.

An app provider may only collect and process as much data from users as is absolutely necessary to fulfil the specified purpose (e.g. use of the app). If the app provider wishes to collect or process more data, it may do so only if the users have consented to this extended data processing. Data which is no longer required must be deleted or anonymised by the app provider.

Ensuring data security

In order for personal data to be processed in accordance with data protection legislation, suitable technical and organisational measures must be taken to ensure risk-appropriate data security.

App manufacturers and providers are obliged to take suitable technical and organisational measures to ensure risk-appropriate data security. Because health apps process sensitive personal data and involve profiling activities, they are subject to relatively high data security risks. The technical and organisational measures taken must therefore satisfy particularly strict requirements.

Safeguarding the rights of data subjects

The data protection legislation provides for a number of rights for data subjects:

- Data subjects are entitled at any time to request information from the data processor about the data concerning them which is being processed.
- If the processed data contains errors, the data subjects are entitled to request rectification of the errors by the data processor.

In order for app users to be able to exercise their rights as data subjects, they must be informed about who is responsible for the data processing – i.e. they must have a contact point where they can assert their rights.

7.3 Need for compliance with EU data protection legislation

Data protection at the EU level

It should also be noted that the new EU data protection legislation has been in force since 25 May 2018. Although this legislation applies primarily to data processing within the EU, it can also apply in exceptional cases to a data processor located outside the EU. This is the case when a data processor offers goods or services to persons who are in the EU and processes personal data concerning the persons to whom the goods or services are offered.

If app developers based in Switzerland also offer an app to persons located in the EU and process data concerning these persons in this context, then the developers are subject to the EU data protection legislation.

It is important to be aware of this fact since the EU data protection legislation in some cases involves stricter processing requirements than Swiss data protection legislation. Moreover, violations may result in substantial fines (running into tens of millions). Thus, whenever apps are also made available in the EU and personal data is processed concerning persons to whom the app is offered in the EU, an in-depth clarification of the legal situation is highly recommended. The EU has produced guidance for the development of mobile health apps. The guidance (Privacy Code of Conduct), together with additional information, can be found here.

Case-by-case analysis essential

Finally, it should be noted that this discussion is no substitute for in-depth analysis on a case-by-case basis. Depending on the circumstances, it may be advisable to consult a data protection specialist.

8 DiGA – Digital Health Applications

8.1 The key facts in brief

In Germany, the Digital Healthcare Act (DVG) introduced the 'app on prescription'. Digital health applications (DiGAs) are apps, desktop or browser applications that are prescribed by physicians and psychotherapists and are reimbursed by health insurers. In order to be included in the DiGA directory of reimbursable apps, the apps must have successfully completed a fast-track assessment procedure of the German Federal Institute for Drugs and Medical Devices (BfArM). The requirements for DiGAs in this assessment are comprehensive and go beyond those that apply to medical software. For example, strict requirements must be met for data protection, information security and interoperability. Furthermore, final listing in the DiGA directory requires evidence of positive healthcare effects of the DiGA by means of a comparative study.

8.2 What are DiGAs?

Across Europe, various approaches and implementations exist for advancing digitisation in healthcare. For example, the EU Commission is working on a legal framework for digital transformation in all EU member states that also includes requirements for medical devices. At national level, various projects have been implemented, including electronic patient records and prescriptions.

App on prescription

In Germany, the Digital Healthcare Act (DVG) introduced the 'app on prescription'. Digital health applications (DiGAs), which can be apps on a smartphone, or desktop or browser applications, are prescribed by physicians and psychotherapists and reimbursed by health insurers. Such applications must have successfully completed an assessment procedure of the German Federal Institute for Drugs and Medical Devices (BfArM) and be listed in the DiGA directory.

Prerequisites

In order to be listed in the DiGA directory, the apps must possess certain qualities. Currently, only medical devices in Classes I and IIa according to the MDR (or MDD during the transitional period) are authorised. In view of the trend towards the stricter classification of software under the MDR, this restriction will be lifted in future, where possible. The medical purpose of the app must be achieved primarily through the main digital function. This requirement rules out software that exclusively controls or collects data from another medical device. A DiGA supports the recognition, monitoring, treatment or alleviation of diseases, or the recognition, treatment or alleviation of,

or compensation for, injuries or disabilities. Apps intended for primary prevention (prevention of diseases in people who are not ill) are excluded. By contrast, functions for secondary (prevention of a deterioration of a disease state) and tertiary prevention (avoidance of secondary diseases or complications) are contained within the term 'treatment' and can be part of a DiGA. Furthermore, DiGAs must always be used by the patient (alone or together with the service providers), and not by the physician for treating patients. A DiGA can also be operated together with hardware, if data is obtained from a smartwatch for example.

8.3 The DiGA directory

BfArM DiGA Directory

The DiGA directory lists all DiGAs that have successfully completed the assessment procedure and that are reimbursed by the health insurer. The directory provides transparent and comprehensive information about the performance and characteristics of DiGAs for patients and service providers, but is also designed to enhance the integration of DiGAs in the structures and processes of healthcare on technical, organisational and practical levels.

The directory provides basic data on the medical device (product name, notified body involved, intended purpose and instructions for use, manufacturer's liability insurance incl. sum insured, etc.), information for the insured and patients (objective, operating principle, content, functions and usage of the DiGA, checklists on data protection and quality requirements, locations where the data is processed and any incurred additional costs for optional accessories), information for service providers (patient group/indication, positive healthcare effects, classification in the healthcare pathway, recommended duration of usage, explanation of the intended user roles, etc.), information for healthcare professionals (study report proving the positive healthcare effects, medical establishments and organisations that are involved, etc.) as well as technical information (confirmation of compatibility regarding supported platforms and devices, standards and profiles used for data exchange).

Provisional and final listing

Manufacturers can apply for the provisional or final listing of their applications in the DiGA directory. For a final listing in the DiGA directory, a comparative study proving a positive healthcare effect must be submitted.

If such a study has not yet been successfully completed but the requirements are otherwise fulfilled, manufacturers can apply for a provisional listing, where the DiGA is included in the directory and is also already fully reimbursable. After 12 months, the manufacturer must have completed the comparative study proving positive healthcare effects, although the trial period can be extended for a further 12 months in isolated cases. The BfArM reviews the results and decides on the final listing of the DiGA within 3 months. In the event of a negative decision, the DiGA is removed from the directory, and the manufacturer can submit a further application for final listing only after 12 months and only after a study has been successfully completed (a second provisional listing is no longer possible).

Application procedure

The application procedure for DiGAs is conducted via the BfArM application portal. As soon as all the mandatory information and associated documents have been submitted online, the BfArM checks the formal completeness of the application. If all the information is complete, the BfArM informs the applicant accordingly within 14 days and confirms the date of receipt as the start of the processing period. If the documentation is incomplete, the applicant is given up to three months to add the missing information to the application. The start of the maximum 3-month processing period starts on the date of receipt of the complete documentation. During the evaluation, the BfArM can request further documents or clarifications and specifies a deadline for the reply, although the 3-month evaluation period is not extended as a result, in other words all the requested information must be submitted within this period.

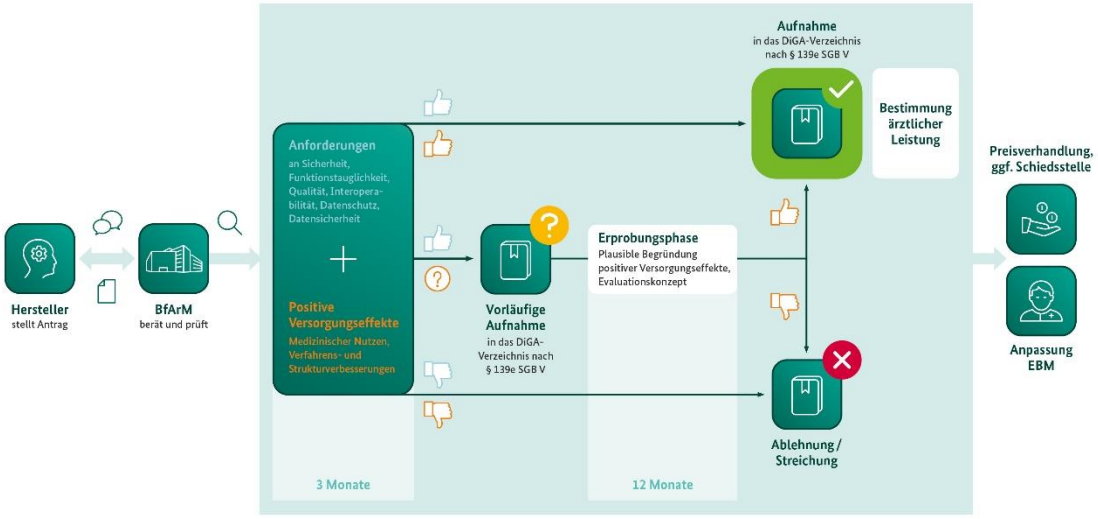


Figure 5: Sequence of the DiGA fast-track procedure. Source: BfArM

8.4 Requirements for DiGAs and manufacturers

DiGA Ordinance DiGAV

The requirements for a DiGA are stipulated in sections 3 to 6 of the DiGA Ordinance (DiGAV). These concern safety and suitability for use, data protection and information security, as well as quality and interoperability. The fulfilment of these requirements is confirmed by means of checklists in the annexes to the DiGAV and corresponding documentation.

8.4.1 Safety and suitability for use

Device safety and suitability for use are considered to have been proven by the certificate of conformity/CE certificate issued by the notified body or the manufacturer's declaration of conformity. This means that medical software that has legally been placed on the market in accordance with the requirements of the MDR satisfies these criteria. As a rule, the BfArM does not carry out any further checks.

8.4.2 Data protection

DiGAV specifies and supplements the requirements of the European General Data Protection Regulation (GDPR) and the German Data Protection Act (BDSG) and Social Code (SGB). The checklist in Annex 1 to the DiGAV contains 40 statements on the technical implementation and on the organisation of the manufacturer and its processes. In particular, these specify or restrict the permitted purposes of the data processing and the admissibility of the data processing outside Germany.

Permitted purposes of data processing

In general, data obtained from a DiGA may be processed only with the express consent of the users. Exceptions from this rule are permitted only if this is permitted or ordered by other legislation, e.g. for invoicing the health insurer by the DiGA manufacturer and to satisfy the requirements of the MDR (traceability of devices, etc.). Data may be processed only for the following purposes:

- To guarantee the correct use of the DiGA by the user
- To prove positive healthcare effects in connection with provisional listing in the DiGA directory
- To provide verification in connection with price agreements between health insurers and DiGA manufacturers
- To permanently guarantee the technical functionality, ease of use and further development of the DiGA

The processing of data for other, e.g. promotional, purposes, is prohibited.

Location of data processing

The data may be processed only in Germany itself, in member states of the EU and EEA, in Switzerland and in third countries with a comparable level of protection (adequacy decision according to Article 45 GDPR). Data processing in the USA for example is not permitted.

8.4.3 Information security

DiGAV also stipulates requirements concerning information security, i.e. the protection of confidentiality, integrity and availability of all data processed via a DiGA. These requirements are based on publications and recommendations of the Federal Office for Information Security (BSI), particularly the BSI Standards 200-1, 200-2 and 200-3.

Certified Information Security Management System (ISMS)

All manufacturers of DiGAs must have an Information Security Management System (ISMS) according to ISO 27001 or BSI Standard 200-2: implement IT basic protection methodology and be certified by an accredited body. This requires the following processes in particular:

- Protection requirements analysis: Continuous process for determining the protection requirements for data, applications, systems, etc.
- Release, change and configuration management: Evaluation of software updates and releases in relation to the re-evaluation of protective measures and risks

- Penetration tests: Simulation of possible attack patterns in order to identify possible security loopholes based on the BSI penetration tests and the OWASP Top 10 Security Risks.
- Directories of libraries used and market monitoring: List of products of third parties used in the DiGA (including open source) and process in order to obtain and evaluate security-relevant, device-related information

The data protection requirements listed in the checklists (Annex to DiGAV) are derived directly from the BSI IT Basic Protection lists of requirements. The following components from the BSI IT Basic Protection Compendium in particular should be taken into account:

BSI IT Basic Protection Compendium

- APP.1.4: Mobile applications (Apps)
- APP.3.1: Web applications
- SYS.4.4: General IoT device

For DiGAs with a very high need for protection (determined by the protection requirements analysis), additional measures are also needed, e.g. the encryption of data on servers and 2-factor authentication for accessing health data.

DiGAs with a very high need for protection

8.4.4 Interoperability

Another requirement for a DiGA is interoperability. This refers to the ability of technical systems to work together at technical-syntactical (exchangeability of data over networks in a specific data format), semantic (common understanding of information by sender and recipient) and organisational (social and legal framework) levels.

DiGAV specifies the interfaces that must be interoperable and how this must be achieved by using standards.

The following interoperable interfaces, in particular, are required:

Interoperable interfaces

- It must be possible to obtain therapy-relevant extracts of the collected data in human-readable and printable form
- It must be possible to obtain collected data in a machine-readable, interoperable format so that it can be processed by other digital products.
- If the DiGA obtains data from other medical devices or sensors (wearables), it must also be able to address these devices via an interoperable interface.

The interfaces concerned may be redundant, i.e. as well as the interoperable interfaces, other interfaces with the same purpose may also exist.

Medical information objects (MIOs)

In order to guarantee the interoperability of an interface, manufacturers can use what are termed "medical information objects" (MIOs). The MIO DiGA Toolkit, a modular medical data structure, is provided and developed by the German Association for Statutory Health Insurance Physicians (KBV). Basically, interoperable interfaces must be implemented using such MIOs. If a corresponding MIO is not available, existing open, internationally recognised interfaces and/or semantic standards can also be used (HL7, ISO, NEMA, etc.).

8.4.5 Further quality requirements

In addition to interoperability, DiGAs must also satisfy further quality requirements.

Robustness

If possible, it must be possible to use DiGAs without interference, loss of data, transmission errors or difficulties connecting with devices. For example, the manufacturer must ensure that power failures or interruptions in the internet connection do not lead to the loss or corruption of data. However, offline usability is not mandatory. External devices and sensors must, where possible, be checked by the DiGA for their proper functioning. Plausibility checks during data entry by the user are also stipulated.

Consumer protection

Manufacturers must inform the users as transparently as possible about the intended purpose and functionality of DiGAs. Compatibility assurances relating to hardware and software must also be given on distribution platforms, and it must be clearly apparent which features are provided by the DiGA and, if applicable, which functions need to be purchased additionally. Although in-app purchases of additional functions, i.e. functions not belonging to the DiGA, are permitted in principle, they may not e.g. be advertised in the DiGA, and they may not be automatically renewable subscriptions or time-limited special offers.
Users' questions must be answered promptly by the manufacturer. Specifically, queries must be acknowledged within 24 hours, ideally with an answer during this period.

Ease of use

The ease of use must be evaluated by means of tests in focus groups, which must also include participants with little prior

experience in handling digital media. In order to guarantee accessibility, DiGAs must either include operating aids for people with disabilities or support the operating aids offered by the platform.

Support for healthcare providers

If the DiGA is intended to be used jointly by users and healthcare providers, the manufacturer must provide clear guidance on which role the healthcare providers fulfils, how this is to be structured in practice and which legal requirements are to be observed in the process.

Quality of medical content

The medical professional basis of a DiGA must be derived from accepted and reliable sources (medical guidelines, established textbooks, published studies, etc.). These sources must be disclosed in the actual DiGA. By means of appropriate processes, the manufacturer must also ensure that this professional basis remains up to date and appropriate and take account of changes in the further development of the DiGA (see section **Fehler! Verweisquelle konnte nicht gefunden werden.** on post-market surveillance).

Patient safety

For ensuring patient safety, and in addition to the technical safety ensured by CE marking, DiGAV also stipulates additional requirements, which are particularly aimed at the conscious handling of existing residual risks for the users. Thus, for example, information must be provided about risks and the appropriate measures to mitigate or avoid such risks. Critical measured values or analytical results must be identified by the DiGA, and the user must be informed of these by appropriate means (reference to a visit to the physician or recommendation to discontinue or change the use of the DiGA). Furthermore, all of the data entered by the user or collected via connected medical devices or sensors must be checked for consistency conditions.

8.5 Evidence of positive healthcare effects

For a final listing in the DiGA directory, the positive healthcare effects (PHEs) of the DiGA must be proved by means of a comparative study.

Positive healthcare effects (PHEs)

Positive healthcare effects are either a medical benefit (MB) or patient-relevant improvements in structures and processes (PISP) in healthcare. Medical benefit is defined as an improvement in the state of health, a shortening of the duration of a disease, a prolongation of survival or an improvement in the quality of life. Patient-relevant

improvements in structures and processes can be achieved in areas such as the coordination of treatment procedures, the alignment of treatment with guidelines and recognised standards, adherence, facilitating access to care, patient safety, health literacy, patient autonomy, coping with illness-related difficulties in everyday life or reducing treatment-related efforts and stresses for patients and their relatives.

Positive healthcare effects must always be achieved in relation to a specific patient group (indication) according to ICD-10 coding. Although a DiGA can be used for several indications, the evidence of PHEs must then be listed separately for each patient group as a rule.

Study proving the PHEs

A study for proving positive healthcare effects usually needs to demonstrate that the use of the DiGA is better for patients than its non-use. This means that the study must show that, for a patient group using the DiGA as part of therapy, a PHE is achieved compared to a comparison group that does not use the DiGA (comparative study). The comparison group can either receive a treatment without the use of the DiGA, not be treated or receive a treatment with another, comparable DiGA.

The studies can be clinical or epidemiological in nature depending on the investigated endpoints, but they can also be conducted using methods of healthcare research, social research or behavioural research, etc. Specific requirements relating to study types and designs can be found in the BfArM DiGA Guide.

The studies must be conducted in Germany and registered in a public study registry. The results of the study must be published no later than 12 months after submission to the BfArM.

Provisional trial listing

Manufacturers that have not yet completed or started a study to prove the PHEs can apply for a provisional trial listing in the DiGA directory. To this end, they are required to submit a systematic data evaluation (literature search and evaluation and evaluation of the data obtained during the use of the DiGA) demonstrating that a PHE can be achieved for a specific patient group. The manufacturer must also submit an evaluation concept with the study protocol. The evaluation concept must be produced by an independent scientific institute, e.g. a Clinical Research Organisation (CRO).

9 MedTech glossary for the app developer

9.1 Legislation and standards

Standard: “Medical devices – Quality management systems – Requirements for regulatory purposes”	ISO 13485
Standard: “Medical device software – Software life cycle processes”	IEC 62304
Standard: “Health software – Part 1: General requirements for product safety”	IEC 82304-1
Standard: “Medical devices – Application of risk management to medical devices”	IEC 14971
European Medical Device Regulation	MDR
Medical Devices Ordinance: Legal provisions for medical devices from Switzerland	MedDO
Therapeutic Products Act: Federal Act on Medicinal Products and Medical Devices	TPA
Human Research Act: Federal Act on Research involving Human Beings	HRA
Harmonised standards	List of harmonised standards

9.2 Authorities, associations, etc.

Swiss Agency for Therapeutic Products (regulatory and supervisory authority for therapeutic products in Switzerland)	Swissmedic
Medical Device Coordination Group (MDCG)	MDCG
International Medical Device Regulators Forum	IMDRF
Example of a notified body	TÜV SÜD
Notified Body Operations Group	NBOG
New Approach Notified and Designated Organisations	Nando

Medicines and Healthcare products Regulatory Agency (UK)	MHRA
Federal Institute for Drugs and Medical Devices (Germany)	BfArM

9.3 Important terminology

Medical devices for medical laboratory testing of samples derived from the human body (**I**n **V**itro **D**iagnostics)	IVD
International Organization for Standardization (responsible for standardization in all areas except telecommunications, electronics and electrical engineering)	ISO
International **E**lectrotechnical **C**ommission (standards organisation in the field of electronics and electrical engineering, e.g. IEC 60601-X)	IEC
Unique **D**evice **I**dentifier (uniform device identification system to ensure traceability) In future, any software/app that is a medical device must also have a UDI.	UDI
Post-**M**arket **S**urveillance (systematic collection of information and evaluation of devices already on the market in order to permit prompt corrective and preventive action to reduce risks)	PMS
Certification procedure that allows manufacturers to prove that their devices fulfil the essential requirements and thus comply with the applicable EU directives	Conformity assessment procedure
General Safety and Performance Requirements. Cf. Annex I to the MDR.	GSPR
Summary of Safety and Clinical Performance	SSCP
Periodic Safety Update Report (PSUR)	Safety Report PSUR

10 Online resources, guides, etc.

Swissmedic – Information on the regulation of medical devices	Swissmedic information
Guide on the implementation of EU products rules 2016 (Blue Guide)	Blue Guide
MEDDEV documents (MDD)	MEDDEV guidance documents
MDCG documents (MDR)	MDCG guidance documents
List of notified bodies accredited under the MDR	List of notified bodies (MDR)
Swiss Association for Standardization (SNV)	Swiss Association for Standardization
BfArM information on placing medical devices on the market	Overview: Placing medical devices on the market
BfArM – Digital Health Applications DiGA	DiGA

10.1 Links, blogs, etc. by private providers

The medical devices blog on general and software-specific topics: *medicaldeviceslegal* (e.g. The new General Data Protection Regulation impact on medical devices industry)	medicalesdeviceslegal
Blog focusing on digital health	mobihealthnews
Provider focusing on medical devices that contain software	Johner Institute
News portal focusing on MedTech and new technologies	medgadget