eHealth Suisse

Guide for app developers, manufacturers and distributors

Practical guidance

Bern, 2 June 2020
Legal notice
© eHealth Suisse, Swiss Competence and Coordination Centre of the Confederation and the Cantons

Licence: This document is the property of eHealth Suisse (Swiss Competence and Coordination Centre of the Confederation and the Cantons). The final document will be published via the appropriate information channels under a Creative Commons Attribution-ShareAlike 4.0 International licence. Licence text: http://creativecommons.org/licenses/by-sa/4.0

Identification of this document
OID: 2.16.756.5.30.1.127.1.3.5.1.1

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>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Basic principles</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Medical software under the MDR</td>
<td>21</td>
</tr>
<tr>
<td>4</td>
<td>Is agile development possible for MedTech?</td>
<td>37</td>
</tr>
<tr>
<td>5</td>
<td>Cybersecurity</td>
<td>39</td>
</tr>
<tr>
<td>6</td>
<td>Legal basis for data protection and security in Switzerland</td>
<td>45</td>
</tr>
<tr>
<td>7</td>
<td>MedTech glossary for app developers</td>
<td>49</td>
</tr>
<tr>
<td>8</td>
<td>Online resources, guides, etc.</td>
<td>51</td>
</tr>
</tbody>
</table>
1  Introduction

1.1  Background
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. As an adaptation to the European Medical Regulation, this definition corresponds to the pan-European legal framework for medical devices. 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. Due to the revision of the European Medical Regulations, medical devices will be more strictly regulated in future and medical software will be assigned to a higher risk class in many cases. 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, MEDDEV 2.1/6). 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?

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

1Medical device means any instrument, apparatus, appliance, software, implant, reagent, material or other articles:
   a. intended by the manufacturer to be used for 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 (alone or in combination) to:
      1. diagnose, prevent, monitor, treat or alleviate diseases,
      2. diagnose, monitor, treat or alleviate injuries or disabilities, or compensate handicaps,
      3. investigate or modify the anatomy, to replace parts thereof, or to investigate, modify or replace a physiological or pathological process or state,
4. providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means

The following products shall also be deemed to be medical devices:

a. devices for the control or support of conception,

b. products specifically intended for the cleaning, disinfection or sterilisation of devices

Medical devices are divided into:

- 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.

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

- “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 Switzerland

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 essential requirements and they must be able to provide verification at any time.

Switzerland has concluded international treaties with the EU member states, the EFTA states and Turkey on the mutual recognition of conformity assessments for medical devices (bilateral agreements or mutual recognition agreements/MRA). These treaties are based on implementation of the European medical device directives and the European CE marking. The signatory states recognise certificates from the Swiss conformity assessment bodies. Conversely, Switzerland recognises conformity assessments produced by notified bodies or conformity assessment bodies in the signatory states.

These treaties simplify the reporting obligations of companies placing products on the market and allow direct sales from Switzerland to all EU and EFTA member states as well as to Turkey – without an authorised representative based in these countries. Conversely, companies based in the signatory states can sell compliant medical devices directly in Switzerland. Notwithstanding the above, the country-specific requirements concerning medical devices continue to apply in the individual signatory states (e.g. reporting requirements for new products, requirements on mandatory languages for product information, regulations on prescription requirements, professional use of products, requirements for distribution channels, points of sale to the public, advertising, reimbursement by social insurance schemes).

The most important legal foundations in Switzerland are as follows:
- Federal Act on Medicinal Products and Medical Devices
- Medical Devices Ordinance
- Federal Act on Research involving Human Beings
- Ordinance on Clinical Trials in Human Research

These legal texts transpose the requirements of the European medical device directives into Swiss law and describe additional
national regulations. Swissmedic and the cantonal authorities are responsible for the enforcement of the Therapeutic Products Act. Here, you can find further information about the bilateral agreements from the FDFA.

2.4 Legal foundations in Europe

At the European level, medical devices are currently regulated by three different directives:
- Medical Device Directive
- In Vitro Diagnostic Medical Device Directive
- Active Implantable Medical Device Directive

In May 2017, the new Medical Device Regulation (MDR) and In Vitro Medical Device Regulation (IVDR) came into force. The MDR will replace the existing MDD and AIMD directives, while the IVDR will replace the IVDD. An implementation period of 3 years (MDR) and 5 years (IVDR) was agreed upon. As a result of the coronavirus crisis, the European Parliament in April 2020 accepted the Commission’s proposal to postpone the date of application of the MDR by one year, until 26 May 2021.

The AIMD is being repealed and integrated into the MDR. The revision of the existing European medical device, IVD and AIMD directives entails major changes and challenges for manufacturers, distributors, suppliers, etc. All products must be newly certified under the MDR (no grandfathering), there are new classification rules (e.g. for software and nanotechnology), and the requirements for clinical data, post-market surveillance, etc. will increase significantly.

The most important changes include:
- Technical documentation must be prepared in much greater detail.
- All medical devices must have a unique device identifier (UDI).
- Every company must designate a person responsible for regulatory compliance (PRRC) who possesses appropriate expertise in the field of medical devices.
- A more detailed clinical evaluation is required, including post-market surveillance data for an update.
- There are new classification rules (e.g. for nanotechnology).
- The classification of some products is also changing (e.g. many software products are being upgraded from class I to class IIa).
2.5 When is software a medical device?

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.

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.

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 2.1/6 offers the most comprehensive aid for deciding whether stand-alone software is a medical device.

Working groups affiliated with the European Commission create MEDical DEVices (MEDDEV) guidance documents. Although these documents are not legally binding, they do provide guidance and assistance in interpreting the MDD, AIMD and IVDD.

For stand-alone software, MEDDEV 2.1/6 provides criteria and examples for the qualification of stand-alone software as a medical device in accordance with the MDD and IVDD.

A flowchart included in the document is useful for the decision-making process:
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 publishes decisions on borderline cases that are important for purposes of interpretation. The latest version of the manual includes various examples of medical apps to aid decision-making.

**2.6 What if my software is not a medical device?**

If software does not satisfy the MDD definition of a medical device and cannot be qualified as a medical device based on the MEDDEV 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.

2.7 Risk classes for medical devices

![Fig. 2 EU MD and IVD risk classes (source: MedTech Europe)](image)

In Europe, medical devices are divided into four risk classes: classical medical devices fall into Classes I, IIa, IIb and III in accordance with Annex IX of Directive 93/42/EEC (or Annex VIII of 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.

![Fig. 3 Directive 93/42/EEC concerning medical devices (Article 9)](image)

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

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:
### 2.8 Certification of medical devices

In order to place a medical device on the market, it must comply with all applicable EU directives and have successfully undergone 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, Switzerland or Turkey and has the applicable product group within its scope.

Information about notified bodies can be found in the Nando (New Approach Notified and Designated Organisations) information system. A treaty between the Swiss Confederation and the European Community regulates the mutual recognition of conformity assessments. The relevant requirements and procedures are specified in various directives and guidelines issued by the EU Notified Body Operations Group (NBOG).

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 and devices for self-testing)

The manufacturer bears sole responsibility for ensuring that its products comply with the essential requirements and the applicable EU directives.

The MDD defines the essential 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 MDD. Essential requirements include, for example:
- Risk management to ensure a favourable benefit/risk ratio
- Proof of electrical or mechanical safety
- Usability
- …

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), introduced under the MDR
- Class IIa, IIb and III medical devices
- Active implantable medical devices
- In vitro diagnostic medical devices as defined in Annex II to Directive 98/79/EC
- In vitro diagnostic medical devices for self-testing

Depending on the classification and intended purpose of the device (see Section 2.5), 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. In addition, the manufacturer receives the appropriate CE certificate. The manufacturer can now place its products on the market in compliance with the regulations.
As mentioned, the conformity assessment procedures differ according to the risk class. The UK MHRA has published an overview of the various procedures here.

Under the MDR (the new regulation), the various conformity assessment procedures are changing. TÜV SÜD has published an overview of the new procedures.

2.9 Relevant standards

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.

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.

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:

*Fig. 5: Relationship between regulations and standards (source: ISS AG)*

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

Development in accordance with IEC 62304 can in principle be implemented using agile development methods, but in practice it involves certain requirements which are difficult to fulfil with a purely agile process.
2.9.3 IEC 62366-1:2015 Application of usability engineering to medical devices

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 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 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.).
IEC 82304-1:2016 Health software – Part 1: General requirements for product safety

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).
3 Medical software under the MDR

The transitional period of the new European Medical Device Regulation (MDR) ends on 26 May 2021. The MDR brings a number of significant changes which need to be taken into account, in particular, by manufacturers of medical software (medical device software, MDSW). Because of the coronavirus crisis, the European Commission proposed that the date of application of the MDR should be postponed by 12 months, with the current legal framework being retained. This proposal was submitted to the European Parliament and Council on 3 April 2020 and adopted at the end of April.

3.1 Qualification and classification

While the basic definition which determines whether or not software is a medical device is largely unchanged, the MDR brings significant changes to the risk classification of medical software. A large proportion of the software 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 the introduction of Rule 11 in Annex VIII to the MDR (Classification Rules).

3.1.1 Classification according to Rule 11

In the MDD, medical software is 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, 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. It states that:

Software intended to provide information which is used to take decisions with diagnosis 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 of 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.

3.1.2 EU MDCG Guidance

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). The thematic content of this document is very similar to that of MEDDEV 2.1/6, but it is now specifically adapted to the MDR. Although this document is not legally binding, it does have considerable weight. 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.

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).
The decision diagram and the associated questions providing assistance with the qualification of software as a medical device were largely taken from the MEDDEV 2.1/6 document (see Section 2.5).

![Decision Steps Diagram](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.
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 information 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.

### 3.1.3 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.
Likewise not to be underestimated is the current scarcity of notified bodies already accredited under the MDR. While 55 notified bodies are accredited under the MDD, only 14 are so far accredited under the MDR (as of June 2020; the updated list is available here). Given this scarcity, lengthy waiting periods are to be expected and forward planning is therefore to be recommended.

The second corrigendum to the MDR, published in the Official Journal of the European Union on 29 December 2019 (and thus legally binding), includes an amendment to Article 120(3), regulating the transitional period. This Article was amended as follows:

*By way of derogation from Article 5 of this Regulation, a device which is a class I device pursuant to Directive 93/42/EEC, for which the declaration of conformity was drawn up prior to 26 May 2020 and for which the conformity assessment procedure pursuant to this Regulation requires the involvement of a notified body, or which has a certificate that was issued in accordance with Directive 90/385/EEC or Directive 93/42/EEC and that is valid by virtue of paragraph 2 of this Article, may be placed on the market or put into service until 26 May 2024, provided that from 26 May 2020 it continues ...*

*N.B.* The decision to postpone the date of application of the MDR until 26 May 2021, on account of the coronavirus crisis, also affects the above Article.

In other words, a device which is a Class I device under the MDD, and which is to be assigned to a higher risk class in accordance with the classification rules of the MDR – as will frequently be 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 device.

In addition, the requirements of the MDR concerning post-market surveillance and vigilance must be complied with.

### 3.2 European database on medical devices (EUDAMED)

Another important new development associated with the MDR is the establishment of the European 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).](image)

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

Data entry and date of introduction

EUDAMED was originally to be introduced in stages from May 2020, at the end of the MDR transitional period. However, introduction of the system has been postponed until May 2022, at which point all the modules are to be introduced simultaneously.

3.3 Clinical evaluation
Under the MDR, as previously under the MDD, manufacturers of medical devices are required to carry out a clinical evaluation for all their devices – irrespective of the risk classification. The main
objective of this process is to demonstrate the safety, performance and 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.

3.3.1 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 for 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.

3.3.2 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.

### 3.3.3 Clinical evaluation of software

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.

3.4 Post-market surveillance 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.

3.4.1 Regulatory basis

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 3.3);
– 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 (see Section 3.4.5).

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.

### 3.4.2 Post-market 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.

3.4.3 Periodic safety update report

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.
3.4.4 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.

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.

3.4.5 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.

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.
4 Is agile development possible for MedTech?

4.1 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.

4.2 Agile development process

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.

The V-model requires a sequential development process:

![Simplified V-model (graphic: ISS AG)](image)

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.

4.3 Standards

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.

4.3.1 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.
5 Cybersecurity

5.1 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.

Through bilateral treaties, Switzerland has adopted the EU’s conformity assessment and certification systems. This means the Medical Device Directive (MDD) is applicable (as will be the Medical Device Regulation in the near future). Due to the risk-based development approach specified by the MDD for medical devices, 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) and, for the first time, a specific rule in Annex VIII is dedicated to medical software. Rule 11 entails a number of changes for medical software manufacturers, since a new definition has been introduced for software and the new classification rules assign most software products to a higher risk class. A higher risk class implies 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.)

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

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.

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

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.

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 directives, 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; this practice will become stricter under the MDR. The MDD also references IEC 62304. Although it only touches on cybersecurity, this is the only standard to explicitly address this topic (in addition, the new version is expected to contain specific requirements).
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:

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

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.

The French Agency for the Safety of Health Products (ANSM) has established a scientific_committee_on_cybersecurity_for_medical_device_software, which will publish guidance and documents to assist manufacturers. 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).
### Review topic

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the software or system contain software of unknown provenance (SOUP)? Identification of SOUP and software versions used</td>
</tr>
<tr>
<td>Does the software use fixed passwords or keys that are the same on all devices or installations?</td>
</tr>
<tr>
<td>Is the user input validated and restricted to valid ranges? Are the valid ranges defined? Has this been tested?</td>
</tr>
<tr>
<td>Is the communication protected against deliberate or accidental manipulation?</td>
</tr>
<tr>
<td>Are the data formats clearly defined? Is the data protected against changes?</td>
</tr>
</tbody>
</table>

### 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:

#### Objects or processes to be protected

<table>
<thead>
<tr>
<th>Protected object</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient data</td>
<td>Relevant for software that processes/analyses/stores patient data</td>
</tr>
<tr>
<td>Business data</td>
<td>Relevant for software that processes/analyses/stores business data</td>
</tr>
<tr>
<td>Device/system integrity</td>
<td>DoS/ransomware/extortion</td>
</tr>
<tr>
<td>Device/system operation</td>
<td>DoS/ransomware/extortion</td>
</tr>
</tbody>
</table>

#### Attackers

<table>
<thead>
<tr>
<th>Attackers</th>
<th>Motivation</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activist</td>
<td>Ideological</td>
<td>To be defined</td>
</tr>
<tr>
<td>Hacker</td>
<td>Recreational</td>
<td></td>
</tr>
<tr>
<td>Hacker</td>
<td>Commercial</td>
<td></td>
</tr>
<tr>
<td>Competitor</td>
<td>Commercial</td>
<td></td>
</tr>
<tr>
<td>Criminal</td>
<td>Commercial</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Vector Description

<table>
<thead>
<tr>
<th>Vector</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical device interface</td>
<td>USB, serial, network</td>
</tr>
<tr>
<td>Logical device interface</td>
<td>Human interface, machine interface</td>
</tr>
</tbody>
</table>

### Attack vectors

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

<table>
<thead>
<tr>
<th>Concept/principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defence in depth</td>
<td>Security measures are implemented not only at the boundaries of the system but also within the system.</td>
</tr>
<tr>
<td>Least privilege</td>
<td>A process or software component should only have as many rights and privileges as are needed to perform the defined task.</td>
</tr>
<tr>
<td>Minimisation</td>
<td>Only software and services that are required should run on a device; this leads to a reduction in the attack surface.</td>
</tr>
<tr>
<td>Compartmentalisation</td>
<td>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).</td>
</tr>
<tr>
<td>Audit trail</td>
<td>Activities are logged</td>
</tr>
</tbody>
</table>

Adapted from [Fundamental Security Concepts](#)
6 Legal basis for data protection and security in Switzerland

6.1 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. |
|

6.2 Applicability of data protection legislation

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.

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.

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:

- **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).

- **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.**

- **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

---

**Data protection in the area of medical apps**

**Sensitive personal data**

**Consent or legal basis**

**Purpose limitation**

**Data minimisation (proportionality)**
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.

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.

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.
6.3 Need for compliance with EU data protection legislation

It should also be noted that the new EU data protection legislation entered into force on 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.

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.
7 MedTech glossary for app developers

7.1 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

Currently valid European Medical Device Directive
MDD

European Medical Device Regulation valid from 2020
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

7.2 Authorities, associations, etc.

Swiss Agency for Therapeutic Products (regulatory and supervisory authority for therapeutic products in Switzerland)
Swissmedic

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)  
Federal Institute for Drugs and Medical Devices (Germany)  

### 7.3 Important terminology

Medical devices for medical laboratory testing of samples derived from the human body (In Vitro Diagnostics)  

International Organization for Standardization (responsible for standardization in all areas except telecommunications, electronics and electrical engineering)  

International Electrotechnical Commission (standards organisation in the field of electronics and electrical engineering, e.g. IEC 60601-X)  

**Active Implantable Medical Devices**, e.g. pacemakers  

**Unique Device Identifier** (uniform device identification system to ensure traceability) In future, any software/app that is a medical device must also have a UDI.  

**Post-Market Surveillance** (systematic collection of information and evaluation of devices already on the market in order to permit prompt corrective and preventive action to reduce risks)  

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  

Minimum safety and performance requirements that a medical device must fulfil. See also Annex 1 to the MDD/Annex I to the MDR.  

Essential requirements  

General Safety and Performance Requirements. Cf. Annex I to the MDR.  

Summary of Safety and Clinical Performance
8 Online resources, guides, etc.

Guide to the regulation of medical devices

“Blue Guide” on the implementation of EU products rules 2016

MEDDEV documents (MDD)

MDCG documents (MDR)

List of notified bodies accredited under the MDD

List of notified bodies accredited under the MDR

Swiss Association for Standardization (SNV)

MHRA guide

BfArm list of medical devices

BfArM information on market access

BfArM information on differentiation and classification

Swissmedic guide

Blue Guide

Guidance MEDDEVs

MDCG guidance

List of notified bodies (MDD)

List of notified bodies (MDR)

Swiss Association for Standardization

Is your app a medical device? (MHRA)

What are medical devices?

Market access

Guidance on medical apps
8.1 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)

Blog focusing on digital health
Provider focusing on medical devices that contain software
News portal focusing on MedTech and new technologies

medicalesdeviceslegal
mobihealthnews
Johner Institute
medgadget