UNIVERSITY OF TURKU
Turku School of Economics

Current trends of applying ISO 14971:2019 standard for Software as a Service (Saas) -type of medical devices

Information Systems Science

Master's thesis

Author:
Raimo Lantelankallio

Supervisors:
Ph.Lic. Antti Tuomisto
Ph.D., Docent Jani Koskinen

18.3.2026

Turku

Student's statement regarding the use of Artificial Intelligence (AI) for preparing and/or writing this thesis:

☒ **I have not used any AI-based tools.**

☐ **I have used AI-based tools**. Their use is documented in the Appendix. The AI tools were used in a way that complies with academic integrity guidelines.

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

Master's thesis

Subject: Information Systems Science
Author: Raimo Lantelankallio
Title: Current trends of applying ISO 14971:2019 standard for Software as a Service (Saas) -type of medical devices
Supervisors: Ph.Lic. Antti Tuomisto, Ph.D., Docent Jani Koskinen
Number of pages: 73 pages
Date: 18.3.2026

Abstract

The purpose of this thesis was to research possible future trends related to implementing ISO 14971:2019 risk management standard to Software as a Service (Saas) -type of medical devices in EU area. The research study was done by studying the current state of EU medical regulation, guidance and standards. Research papers were reviewed since past five years to find possible future trends. Future trends were searched by analyzing 20 most relevant and recent research papers and collecting key points. Key points were combined and most frequent issues were transformed into possible future trend.

According to this thesis, possible future trends related to implementing ISO 14971:2019 standard to medical software devices are: There is a need for global perspective to medical device regulatory instead of regional and national standards and regulations. The need was identified for alignment for various guidances and standards which typically contain similar issues and similarities. Requirement for better adoption of fast-evolving cybersecurity issues to software medical product was also identified as a possible future trend.

Because of increased need for using AI for processing sensitive data, this could be also a reason to extend ISO 14971 usage from medical device industry to AI applications.

Keywords: MDR, ISO 14971, ISO 16485, risk management, software

Pro gradu -tutkielma

Oppiaine: Tietojärjestelmätiede
Tekijä: Lantelankallio Raimo
Otsikko: ISO 14971:2019 -standardin soveltamisen nykytrendit SaaS-tyyppisissä lääkinnällisissä laitteissa
Ohjaajat: Lehtori, Ph.Lic. Antti Tuomisto, FT dosentti Jani Koskinen
Sivumäärä: 73 sivua
Päivämäärä: 18.3.2026

Tiivistelmä

Tämän opinnäytetyön tarkoituksena oli tutkia mahdollisia tulevaisuuden trendejä, jotka liittyvät ISO 14971:2019-riskienhallintastandardin soveltamiseen SaaS-tyyppisissä lääkinnällisissä laitteissa EU:n alueella. Tutkimus tehtiin tutkimalla EU:n lääketieteellisen sääntelyn, ohjeistuksen ja standardien nykytilaa. Tutkimuspapereita tarkasteltiin viimeisen viiden vuoden ajalta mahdollisten tulevaisuuden trendien löytämiseksi. Tulevaisuuden trendejä etsittiin analysoimalla 20 oleellisinta uusinta tutkimusta ja keräämällä keskeisiä kohtia. Keskeiset kohdat yhdistettiin ja yleisimmät ongelmat muutettiin mahdollisiksi tulevaisuuden trendeiksi.

Tämän opinnäytetyön mukaan lääketieteellisten ohjelmistolaitteiden ISO 14971:2019 -standardin käyttöönotossa mahdollisia tulevaisuuden trendejä ovat: Lääkinnällisten laitteiden sääntelyyn tarvitaan globaali näkökulma alueellisten ja kansallisten standardien ja määräysten sijaan. Tunnistettiin tarve yhdenmukaistaa erilaisia ohjeita ja standardeja, jotka tyypillisesti sisältävät samankaltaisia asioita ja yhtäläisyyksiä. Myös nopeasti kehittyvien kyberturvallisuusasioiden parempi käyttöönotto lääketieteellisten ohjelmistotuotteiden osalta tunnistettiin mahdolliseksi tulevaisuuden trendiksi.

Koska tekoälyn tarve arkaluonteisten tietojen käsittelyssä kasvaa, tämä voisi olla myös syy laajentaa ISO 14971 -standardin käyttöä lääkinnällisten laitteiden teollisuudesta tekoälysovelluksiin.

Avainsanat: MDR, ISO 14971, ISO 16485, risk management, software

TABLE OF CONTENTS

1 Introduction 8

1.1 Motivation 8

1.2 The importance of future trends 9

1.3 The definition of a medical product 10

1.4 Financial aspects of risk management 11

1.5 Typical risks related to general SaaS type of products 12

1.6 Examples of risks related to medical devices 12

2 Background 14

2.1 Medical regulation in EU area 14

2.2 SaaS-type of medical product 15

2.3 Medical device quality management standard ISO 13485 15

2.4 Risk management standard ISO 14971:2019 16

2.5 ISO 14971:2019 and SaaS-type of medical software product 16

2.6 Current state of ISO 14971 risk management in SaaS medical products 18

2.7 EU regulations coming near future related to software medical devices 26

2.8 The relationship of regulation, standards, guidance documents and medical software product 26

2.9 Earlier studies related to the general risk management of medical devices 27

2.10 Conclusion of possible trends derived from recent studies 30

2.11 ISO 14971 convergence with EU AI Act and ISO 42001 30

3 Research question and methodology 32

3.1 Research question 32

3.2 Research methodology 35

3.3 Data collection 35

3.4 Classifying possible future trend from literature review 36

3.5 Limitations of the research 37

3.6 The role of AI in this thesis work 37

3.7 The result of literature search for planned trend study 38

3.8 The discussion related to literature search for planned trend study 38

4 Results 40

4.1 EU regulation and guidance 40

4.1.1 Summary of findings from medical device regulatory 45

4.2 Review of relevant research 45

5 Discussion 53

5.1 List of identified future trends 53

5.2 List of identified trends 56

5.2.1 Global perspective to medical device regulatory 58

5.2.2 The need for alignment for various guidances and standards 58

5.2.3 Better adoption of fast-evolving cybersecurity issues to software medical product 58

5.2.4 Increased automation of risk management -related tasks in the development of medical software 59

6 Conclusion 60

6.1 Possible subjects for further study 62

References 64

FIGURES

Figure 1. The relationship between the regulation and product development 17
Figure 2. The relationship between standards and typical SaaS type of medical software product development 20
Figure 3. General implementation of ISO 14971 risk management 21
Figure 4. The general idea of this thesis for mapping possible future trends. 33
Figure 5. Summary of possible SaaS-type of medical device according to this study. 62

TABLES

Table 1. Review of the history medical software device related standards and guidance documents 23
Table 2. Review of the relevant ongoing EU medical device regulation issues 26
Table 3. Review of past studies on the topic 27
Table 4. Review of recent guidance related to medical device regulation 40
Table 5. Possible future trends 53
Table 6. Possible main future trends 57

1 Introduction

This thesis is about future trends of implementing certain risk management standard to software medical products. Future trends of risk management related issues may help defining possible improvements and for clarifying current problems. Estimating of possible future trends can also help aiming resources in more efficient way. Since the medical device regulation, technology and risk management is constantly changing, it might be good to stop for observing current situations and planning future directions.

1.1 Motivation

Risk management is the heart of medical device regulation. Medical device related regulation aims to identifying and mitigating possible risks to end-users. Medical devices can be various types, ranging from physical products to complex software systems. Because of the increasing number of digital services and data, digitalization megatrend may cause that the number of software products (including medical software products) will emerge in the future (Sitra 2026). Typical software is more often cloud-based software which can be accessed and used as a service where the manufacturer ensures that the software is available and accessible.

The risk management related to physical medical products is easy to understand but complex cloud-based medical software products can be very complex and new unexpected risks can occur since the technology advances rapidly. Although similar risk management methods can be used for detecting and mitigating risks of both physical and software products, types of risks can be very different between physical and software products. The author of this thesis has worked with ISO 13485 quality management standard and ISO 14971 risk management standard in a Finnish software medical device company several years.

To understand the current state and possible future trends of ISO 14971 based risk management, it is important for planning the risk management related activities to understand also possible future trends. Understanding the risk management of software medical products can be very difficult task because it requires understanding the medical regulation itself, product related information and how to apply regulation to the specific medical product. The use of standards ensures that required methods, processes and requirements are defined, implemented and used in a daily work, and there is a common framework for applying for example risk management methods. The use of external auditors will give also a strong signal of regulatory compliance.

To understand risk management implementation, it is essential to understand the environment where cloud-based medical device software is running, how the software is developed and how different risks may affect to the use of the medical software device. The risk management can be either reacting to occurred risks or proactively mapping for possible risks that have not been yet occurred. Since the proactive risk management approach is considered much better (since it is financially more efficient to react problems beforehand) it is also vital to define possible future trends how risk management issues of medical software device may evolve. If future trends are known or predicted, aiming of resources (like the training of personnel, the use of software tools or other similar issues) will be easier. Wrong kind of planning (without knowing future trends) may easily lead to wrong assumptions and causing both financial and patient safety related risks.

Mapping of future trends of medical software risk management is not an easy task since there is no clear information how technological systems will evolve and what kind of exact solutions there will be. However, there is still a possible to detect possible weak signals by analysing recent research papers, extracting possible risk management related trends and summarizing those trends. As a result, this approach provides hints about what kind of issues will be especially important in the near future. By selecting relevant research papers, extracting key points, summarizing those and utilizing author's previous experience related to risk management, it is possible to define future landscape of implementing ISO 14971. If there are some general future trends, those possible trends could be somehow visible in reviewing relevant number of research papers.

1.2 The importance of future trends

There are numerous scientific papers related to mapping future trends (for example Fergnani 2019) where estimating possible future scenarios may bring new information. According to Mazov et al., a literature review including expert verifying the results is a common way of estimating possible future trends (Mazov et al. 2020).

The mapping of possible future trends related to the risk management of medical software device can be valuable in the sense of product development costs - mapping could help reacting to identified issues beforehand and utilize the available information in the product development phase where the costs of managing risks is cheaper than making corrections to existing products with risks.

1.3 The definition of a medical product

This thesis concentrates in EU area because and according to EU regulation, there are certain criteria when a product is defined to be a medical product. If a product fulfils the criterion for a medical product, it is not allowed to use for medical care without filling the EU regulations. Filling EU regulation must be based on filling the official Medical Device Regulation (MDR) (EU 2017) and standards, including the implementation of risk management process and other processes and documentation requirements.

If the product only stores patient data, it is not a medical product. However, if the patient data is altered or the patient data is used for decision making, thus fulfilling the device's intended medical purpose (e.g., diagnosis, prevention, monitoring, treatment, or alleviation of disease), the product may fall into category of a medical device (MDR, Article 2(1)). If device is a medical device and it is used without filling the EU regulation, sanctions may apply. Medical device must also have a CE (Conformité Européenne) mark to show that the product fulfils the EU medical regulation.

Software or part of the software can be also classified as a medical device (Software as a Medical Device, SaMD). The classification is not always straightforward and easy to define and therefore there are many guidance documents such as those published by the Medical Device Coordination Group (MDCG) and other instructions published. The device's risk level is determined via classification rules (I, IIa, IIb, or III), with higher risk devices requiring stricter conformity assessment procedures.

SaaS-type of medical software is a software which is classified as a medical device and the software is used for making decisions related to patient health or healthcare operations done for the patient. SaaS-type of software is executed in cloud environment and typically the software producer guarantees that the software is operational and available for the customer. A key consideration for SaaS/cloud-based medical devices is compliance with cybersecurity requirements within the MDR, as well as the General Data Protection Regulation (GDPR) for handling sensitive patient data. An example of SaaS-type of medical device software is for example cloud-based blood bank software which is operated via browser, and which is used for defining suitable blood products for patients.

An example of a software product which is not classified as a medical device is a system storing unprocessed patient information which is not altered. If the system is disabled, the same patient information can be recorded elsewhere (in paper or spreadsheet). The role of the system is only to automatize the storage of data.

An example of similar system which fulfils the criterion of a medical software is a similar system which has also algorithms which will be used for manipulation of the patient data. Results of algorithms are used for making decisions related to patient health. If the system is disabled, decisions cannot be made without the system or decision making is very difficult. This software is considered as a medical software. Typically, this kind of software may have also other functionalities which are not classified as a medical device but since the existence of medical device features, the software is classified as a medical device if the medical part is not isolated from other functionalities of the software.

1.4 Financial aspects of risk management

The cost of mitigating the risks depends on the phase when the risk is identified and mitigated. If risks are known in the very early stages of product development, the cost is l when compared to risk which is identified and mitigated after the final product has been already delivered to the customer. Cybersecurity, managing sensitive patient data and other similar issues may also cause financial loss if risks related to those are not known and mitigated.

Since medical regulation is constantly expanding, the need for software tools for managing the requirements of ISO 14971 is also increasing. Company processes, updating medical software and other ongoing issues may also increase the need for more careful planning of risk management activities. If changes can be reacted beforehand (proactively), proactive reaction may also affect the financial costs of risk management.

According to Risk Management Association of India, the patient safety and risk management software market is expected to rise by 2030. The main driving factors for growth are rising investments, advancements in technology and increased focus on patient safety (Risk Management Association of India 2025).

MarketsAndMarkets have estimated that the total patient safety and risk software market was around 1.58 billion US dollars in 2024 and will be 2.99 billion US dollars in 2030. The main growth in monetary units will take place in Europe and North America. Fastest-growing region is Asia Pacific according to the forecast. The main growth will be related to cloud-based software (MarketsAndMarkets 2025).

Since the regulation is increasing, the complexity of the medical products is also increasing and software development will be moving to more automatized, the need of software tools for managing ISO 14971 tends to increase. The complexity can be controlled by careful proactive planning of risk

management activities. Increasing complexity may easily lead to also increased need for personnel training.

Implementing risk management processes to medical software production is also a way to reduce possible financial risks. When processes are controlled and there is a plan, it is easy to estimate costs and effects of risk management. Efficient risk management will also reduce possible hazards which may cause extensive costs for the company.

1.5 Typical risks related to general SaaS type of products

Typical risks related to SaaS type of software products are (Ahmadi 2024):

- Vendor lock and portability issues related to transferring data from one product to product manufacturer by other company. This risk is related to the user of the product (not manufacturer's risk). Also, if the service is frequently used and the service is later terminated by the manufacturer, there is a risk of data loss and interruption of the service.
- Regulatory risks related to managing the data. These are risks for the manufacturer related to accessing, storing and processing the user data. Especially patient data must be treated with extra care. Medical device manufacturer must also follow the medical regulations and standards and deviations from those may cause risks (mainly related to financial and reputation related issues).
- Service availability related risks include the availability issues related to providing the service. Typically, there can be an agreement relating how long service interrupts are allowed and possible hostile actors may conduct denial of service attacks to disrupt the service. Also unexpected service and bug fixing may cause unplanned breaks in service availability. Since SaaS product is typically interconnected to other products, service breaks of other products may cause also service breaks is products connected to that.

1.6 Examples of risks related to medical devices

For example, in Finland, a local authority is Fimea (Finnish Medicines Agency) which will ensure that medical devices will meet the regulatory requirements. For example, in 2025, Fimea announced that they will conduct surveillance operations to examine the awareness of medical regulation in medical software companies (Fimea 2025). If the company is not aware of medical regulation, these kinds of surveillance operations can detect such companies.

If the medical software does not work as planned, the patient safety may be endangered. Yle reported in 2020 about incident, where medical software update caused some laboratory examination requests not to be sent. Missing examination requests may delay the patient care (Yle 2020). This kind of problem may be the result of missing risk management actions in installation of medical software updates, possible unseen risks in software testing process or other missing risk management actions.

Risk management of medical software products is not always pure software development issue. Yle reported in 2025 that sensitive patient information was found from the memory device in a local flea market (Yle 2025a). If patient information can be retrieved from a medical software, risk management must be also applied to the patient information exported out of the system. Exporting and managing patient information outside of the system may not be obvious risks for the software itself but it is however a risk which the company must mitigate.

If the device fulfils the definition of the medical device but the device does not meet the regulation requirements, the authorities will try to prevent the use of the device. For example, in 2025 Yle reported that medical devices were sold as a medical device, but devices did not meet the regulation requirements (Yle 2025b).

If the medical software is officially a medical device, the manufacturer must ensure that the device will meet the current regulatory requirements. Yle reported about the software which was used by Finnish medical laboratories and the software did not meet all regulatory requirements (Yle 2023). Although the software mentioned was an old and was about to be replaced with newer software, missing regulatory compliance may cause also financial sanctions.

2 Background

To understand the concept of risk management of medical software products, some key concepts must be discussed. The medical software product must be defined, the regulation related to the medical devices must be addressed and the role of different standards must be understood.

Understanding the risk management of SaaS type of medical software device requires understanding the following concepts:

- EU regulation
- SaaS concept
- Medical device quality management standard
    - including risk management standard
        - implementation of risk management in medical software device product's processes

2.1 Medical regulation in EU area

The medical regulation in EU is based on a regulation related to medical devices (EU 2025a).

The evolution of medical product regulation in EU in brief is (according to Fraser AG et al 2025 and Fimea 2021):

- In 1993, there were many medical related standards and there was a need to harmonize those standards
- The first version of ISO 13458 standard was published in 1996
- The first version if ISO 14971 standard was published in 1998
- The work related to implementing medical device directives begun in 2008
- The Medical Device Regulation 2017/745 was published in 2017 and updated in 2024, including implantable and general medical devices, the roles for supervising the regulation were also defined. Also, regulation for medical devices used for patient samples outside patient (in-vitro) was introduced in 2017.
    - According to medical device regulation, medical device development must have a quality system which includes also a comprehensive risk management

- Medical Device Regulation 2017/745 is in use in EU since 26.5.2021
- Medical devices sold as a medical product must follow the medical regulation

2.2 SaaS-type of medical product

SaaS-type of medical product is a software which is typically installed to cloud. Software is maintained by the software provider. Software updates, bug fixes and other maintenance is done by the software provider, and the software is assessable to the customer to be used. Typically, service level agreement defines desired amount of time which software should be accessible and usable.

Medical software product is a software which is classified as a medical product. This type of software must fulfil appropriate standards and regulations to be sold as a medical product. A good example of SaaS-type of medical software product is a laboratory information system containing parts which are classified as a medical product. The laboratory information system itself can be used only for information storing purposes but if the system manipulates data and that data is used for medical purposes, this part of the system can be classified as a medical product. Laboratory information system can be accessed and used via web browser.

2.3 Medical device quality management standard ISO 13485

Regulation requires that medical device development must follow medical device related quality management standards. Although it is not stated which standard to use, practically ISO 13485 is normally used since there might be no other relevant standards.

ISO 13485 is a quality management standard which can be roughly divided into following parts:

- ensuring that the management is involved in quality management and there are enough resources available and all relevant company processes are described and documents contain version and approval history data
- requirements relating to product development -phase; from collecting customer requirements, implementation and testing, product delivery, service maintenance and collecting used feedback
- risk management is also required to control the whole medical device production process
- measuring the effectiveness of the quality management system and making possible corrective actions when needed

2.4 Risk management standard ISO 14971:2019

According to regulation, medical products must have risk management applied. Risk management is used for identifying and mitigating possible risks related to the use of medical products. Risk management process is ongoing process which is used for defining and collecting known and foreseeable risks. When risks are identified, the usage leading to risk occurrence is defined and outcome of risk. Risk severity and probability will be classified, and possible mitigation actions will be defined. Mitigations may include various types of implementations. Risks can be mitigated in early development phase; bug fixes can be used for mitigating risks and users can be trained to avoid risks.

ISO 14971 standard contains roughly following parts:

- risk identification
- identification of circumstances which may lead to risk
- harm caused by the risk
    - severity
    - probability
- possible risk mitigation
- risk severity after the mitigation (typically mitigation affects only severity, and the probability stays the same)
- possible identification of possible new risk(s) caused by mitigation
- observing the effects of risk mitigations, searching for possible new risks and making necessary changes

2.5 ISO 14971:2019 and SaaS-type of medical software product

Typically, ISO 14971 standard is used as a framework for risk management for medical software products. Medical device manufacturers must have appropriate risk management process which must fulfil the requirements for ISO 14971 standards. Risk management actions should be included in all relevant company processes to identify and mitigate risk efficiently. The general idea of

relationships between regulation, standards and product development is shown in the Figure 1 below.

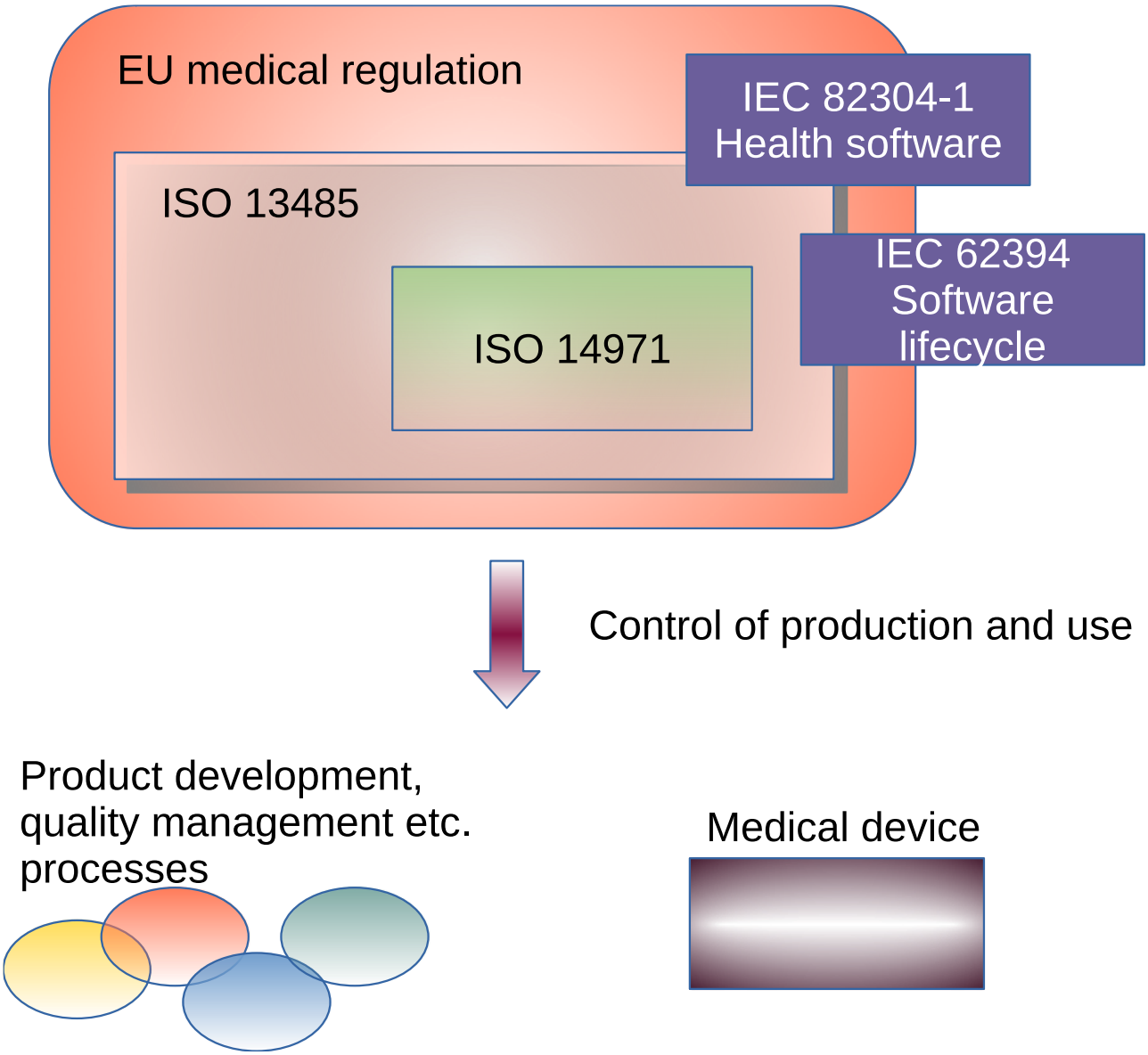

Figure 1. The relationship between the regulation and product development

Typical cybersecurity risks can be divided into CIA -triad; confidentiality, integrity and accessibility (NIST 2024):

- confidentiality -related
    - for example, ensuring that confident data remains confident and the data is not used for unauthorized purposes and the data is not manipulated

    - for medical software case, there is patient and health related data which must be accessible for patients only and persons with special access.

- accessibility -related
    - for example, the service is accessible and can be used, also possible changes to interconnected services are managed and service is not interrupted even if some changes or updates are made to the system or interconnected systems
    - for medical software case, the medical software running on cloud (SaaS) must be accessible to users and other persons who need an access to the service
- identity -related
    - for example, user using the system can be identified via different types of identification methods
    - medical software must have proper authentication methods for identifying users

These main principles of cybersecurity issues can be also applied to SaaS-type of medical product and the risk management of SaaS.

Risk management standard must be applied to SaaS-type of medical product. Risk management of SaaS-type of medical product is used for making the use of the product safer. Typical viewpoints of risk management of SaaS-type of medical products are:

- risks related especially to the network usage and accessibility of SaaS
- possible risks and compatibility issues related to interfaces to different systems
- cybersecurity issues
- tools and software related to risk management of SaaS
- managing of identification and access rights of users of SaaS
- protecting health related data

2.6 Current state of ISO 14971 risk management in SaaS medical products

An official guidance document from the Medical Device Coordination Group (MDCG) endorsed by the European Commission has been published for the companies producing medical device

software. The contents of the document will be about demonstrating compliance with EU MDR Annex I General Safety and Performance Requirements (GSPRs) as they relate to cybersecurity. The guidance document introduces some basic cybersecurity issues which also include the misuse of the product. According to the guidance document, the safe design of the medical device starts from the design phase where risks are identified. After the product is set to the market, the post market surveillance will be done to monitor for existing risks and detecting possible new and emerging risks. MDR and IVDR annexes defines certain cybersecurity -related issues which must be considered when producing medical software products (EU 2019, EU 2017).

Figure 2 below illustrates how EU regulation and standards affect to company processes. The company must ensure that company processes are designed according to regulatory requirements. For example, risk management issues must be taken into account in several company processes, starting from designing phase to implementation and testing, product delivery to customer and maintenance.

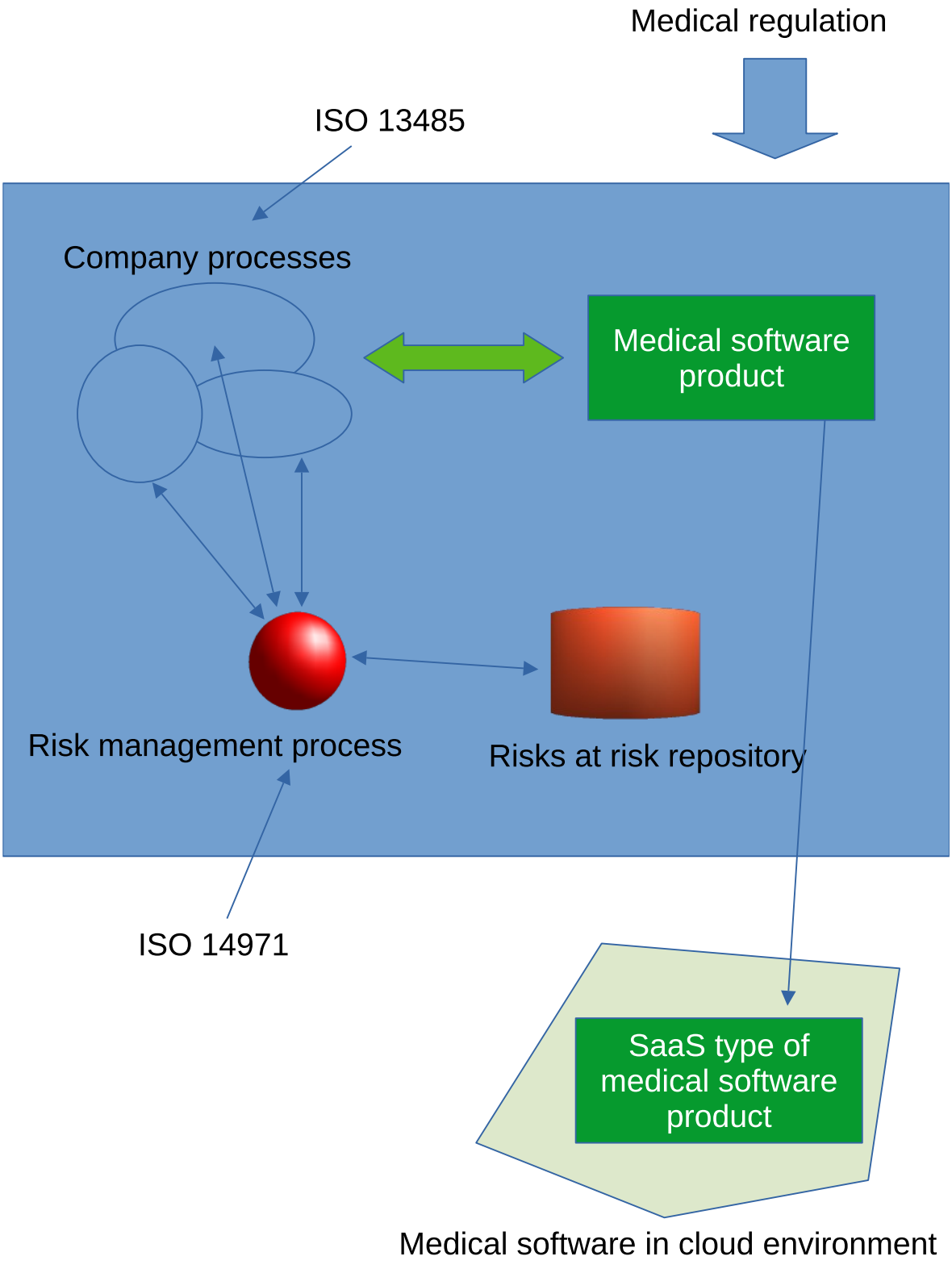

Figure 2. The relationship between standards and typical SaaS type of medical software product development

Typical risk management implementation is shown in the figure 3 below. Typically, medical device manufacturing company has several processes which have connections to risk management and risk management issues are interconnected between all processes.

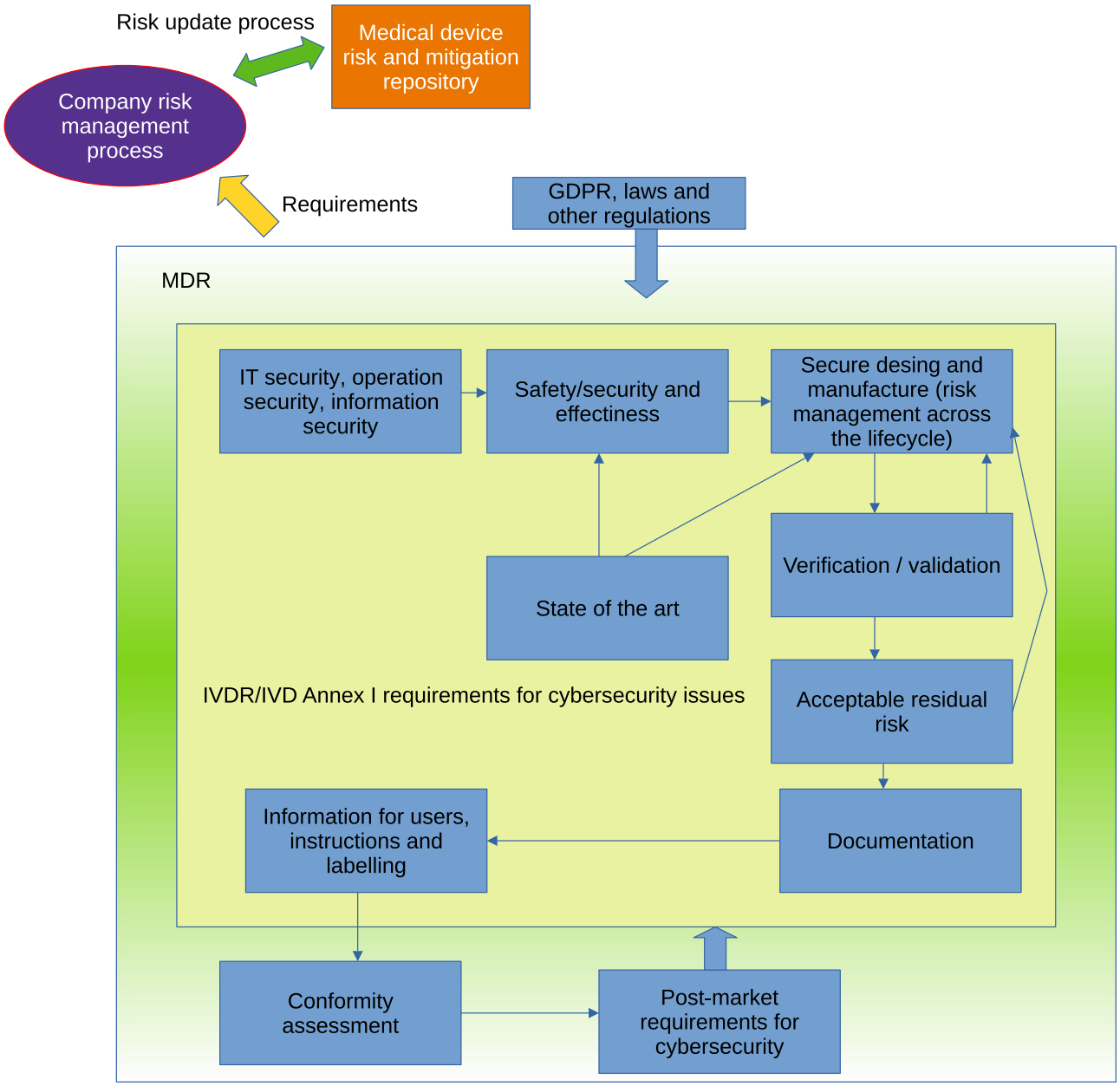

Figure 3. General implementation of ISO 14971 risk management

This guidance document has been a baseline for other publications, blogs and other similar report. For example, a post from I3CGlobal is about integrating especially cybersecurity risk management in product's risk management lifecycle (I3CGlobal 2025).

Also, earlier posts and documents emphasize the fact that the risk management process should be continuous and dynamic (for example C2A Security 2024). The continuous and dynamic risk management process is essential for cybersecurity risk management since it is important to constantly monitor the system for possible vulnerabilities and other similar activities.

There has been also ongoing discussion about the use of artificial intelligence and different kinds of adaption of artificial intelligence (for example AAMI Array 2023). The use of artificial intelligence usually brings own specific problems – like the possibility that the training data is biased and the biased training data will cause medical device software to produce wrong results.

After the guidance document for cybersecurity issues was published (EU 2019), common theme for different blogs was about applying guidance to the product development (for example Medium.com 2021). Since there are many different medical software products, applying guidance, standards and other regulation play a great part of quality related work in companies.

There has also been discussion related regulatory -based risks (for example LFH Regulatory 2025). Regulatory related risks refer to the situation where regulatory requirements are not met, and this may cause problems to the medical device software development company or – in worst case – for the patient. Since the development of the medical software is a continuous process including software releases and updates, the importance of continuous risk management plays a key role in mitigating risks.

Also, discussion has been about breakdown of risk management activities including – for example – calculation of residual risk and risk-benefit analysis (for example Ketryx 2024). Calculation of risk-related issues may be difficult if there are many software releases and the effects of mitigations are difficult to be measured. Also, when there are other partners in SaaS-type of environment, the risk mitigation and risk management in generally should take those partners, connections and other external issues into account.

Also, official new standards have been published related to implementing risk management of medical devices. For example, standard ISO/TR 24971:2020 Medical devices — Guidance on the application of ISO 14971 defines step-by-step instructions on integrating risk management based on ISO 14971 (ISO 2020) and IEC/TR 80002-1:2009 Medical device software Part 1: Guidance on the application of ISO 14971 to medical device software (ISO 2009). Although there are many explanatory standards and instructions, understanding the best practices and specific implementation can be difficult since every medical software product is a bit different and same principles are typically implemented with a bit different ways.

Since the medical device quality management standard is a risk based, the level of risk management also depends on the risk classification of the medical device. Risk classification defines possible risks what the device can cause to the patient. If the device is used directly controlling patient health

issues, the risk class is high. If the device is used only for monitoring and making suggestions related to patient health issues, the device risk class is low. There is a separate guidance related to risk classification of medical device called MDCG 2021-24 - Guidance on classification of medical devices (EU 2021c). When implementing risk management, the risk class of the medical device and risks related to specific parts of the medical software device also affect to the implementation of the risk management.

There is also work done by International Medical Device Regulators Forum (IMDR) about specifying what is exactly a software as a medical device (the definition) and how to apply a risk management to that (IMDR 2015).

The evolution of medical device standards and guidance documents are seen on the table below. The frequency of releasing new guidance or other relevant information is increased during last years. It must be also noted, at the same time, software development tools have been evolving, and the evolution of tools have increased the pressure of releasing new guidance documents.

The table 1 below shows some the general evolution of medical device related standards and EU regulations. Although the table is not complete, the long-term evolution and constant development of standards and regulations can be seen from the Table 1 below.

Table 1. Review of the history medical software device related standards and guidance documents

The table presents an evolution of medical regulation, selected guidance documents and regulation is presented.

Year	Document	Document type	Relationship to risk management
1996	<ISO 13485 first version published>	Standard	Quality management definition
1998	<ISO 14971 first version published>	Standard	Risk management definition
2006	IEC 62304:2006 Medical device software — Software life cycle processes	Standard	Software life cycle issues
2009	IEC/TR 80002-1:2009 Medical device software Part 1: Guidance on the application of ISO 14971 to medical device software	Standard	Guidance about implementing risk management to medical device software
2016	ISO 13485:2016 Medical devices — Quality management systems — Requirements for regulatory purposes	Standard	Current version of quality management standard

Year	Document	Document type	Relationship to risk management
2017	Consolidated text: Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance)	EU medical directive	EU directive defining principles for medical devices
2017	Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.)	EU medical directive related to in vitro diagnostics	EU directive related to in vitro diagnostics related medical products
2019	ISO 14971:2019 Medical devices — Application of risk management to medical devices	Standard	Current version of quality management standard
2019	MDCG 2019-16 - Guidance on Cybersecurity for medical devices.	EU guidance	Cybersecurity risk management issues
2020	ISO/TR 24971:2020 Medical devices — Guidance on the application of ISO 14971	Standard	More specific instructions to implement risk management
2021	MDCG 2021-24 - Guidance on classification of medical devices	EU guidance	Clarified instructions related to the safety classification of medical devices
2022	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	Standard	Cybersecurity standard
2023	Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices (September 2023).	EU guidance	Clarified definition about what is exactly a medical device
2023	Add 1 - MDCG Position Paper on the application of Art.97 MDR to legacy devices for	EU guidance	Guidance related to older medical products whose

Year	Document	Document type	Relationship to risk management
	which the MDD or AIMDD certificate expires before the issuance of a MDR certificate		production began before EU regulation
2023	Update - MDCG 2020-16 Rev.2 - Guidance on Classification Rules for in vitro Diagnostic Medical Devices under Regulation (EU) 2017/746	EU guidance	Updated safety classification for medical devices
2023	MDCG 2023-1 Guidance on the health institution exemption under Article 5(5) of Regulation (EU) 2017/745 and Regulation (EU) 2017/746.	EU guidance	Specifies in-house software product issues. Risk management should be also applied to in-house developed software which fulfills the definition of medical device.
2024	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)	EU AI directive	Directive defining the safe use of AI in medical devices
2025	General Principles of Software Validation; Final Guidance for Industry and FDA Staff	FDA guidance	Guidance related to validating (especially cloud-based) software tools for medical device production
2025	MDCG 2023-3 rev.1 - Questions and Answers on vigilance terms and concepts as outlined in the Regulation (EU) 2017/745 under Regulation (EU) 2017/746 - November 2024	EU guidance	Updated information on how safety incidents should be reported
2025	Proposal for a regulation to simplify rules on medical and in vitro diagnostic devices	EU regulation proposal	Proposal for simplifying the EU medical regulation related to in vitro diagnostic devices

Although to the table, the evolution of medical standards and regulations is ongoing process where additional guidance and principles are being published according to specific needs.

2.7 EU regulations coming near future related to software medical devices

In addition to directives and guidance documents, there are many issues currently ongoing related to medical software safety. It is vital to follow EU actions to maintain the current status of EU medical regulation. Since the regulation is constantly evolving, systematic approach is needed to follow the regulation.

Table 2 below shows some examples of ongoing issues related to EU medical device regulation. The table is not complete, but the table shows some general issues which are currently important.

Table 2. Review of the relevant ongoing EU medical device regulation issues

Article	Scope	Key points
Medical Devices – EUDAMED (EU 2025c)	In-vitro medical devices including software	Registration of medical devices including software for better controlling medical software development roles, software versions and medical device parts of the software
Medical devices –uniform application of the requirements for notified bodies (EU 2025d)	Requirements are being defined for notified bodies which will inspect the regulatory compliance of medical devices	Proposal for requirements related to monitoring the regulatory compliance are being collected.
Extension of the IVDR transitional periods (EU 2024b)	In-vitro diagnostic -type of medical devices are here as an example. Medical devices must meet the regulatory compliance and since there is so-called legacy software, EU has set a deadline when also legacy software must meet EU medical regulation requirements	Certain type (in-vitro diagnostics) of legacy medical software must be regulatory compliant after the transition period. This requires that all regulatory issues, including ISO 149871 risk management implementation, must be met.

2.8 The relationship of regulation, standards, guidance documents and medical software product

The relationship between regulation and the medical software product is

- depending on the purpose of the software product, software or part of it can be classified as a medical product, the risk classification defines the level of risk management
- if software or part of it is classified as a medical product, medical regulation must be fulfilled

- medical regulation set principles for production, for example the use of quality management standard (usually ISO 13485) including risk management (ISO 14971)
- because variety of the medical products, guidance documents are needed to cover and explaining issues
- medical regulation is constantly evolving, software development practices are changing, new technologies will appear so there is a need for constant development of company processes
- for SaaS-type of medical devices, cybersecurity and network issues bring extra aspects to the risk management

Since the regulation is constantly changing and the regulation is difficult to manage, EU published in 2025 proposal for reducing the regulatory burden for in vitro medical devices (EU 2025e).

2.9 Earlier studies related to the general risk management of medical devices

Earlier studies related to thesis subject was searched from Google Scholar by using keywords "medical device risk management". General risk management of all kinds of processes and devices (not limited only to medical devices) has been a constant subject for various research. Typically, medical device related risk management has more regulation than ordinary risk management. Increased regulation causes more work for manufacturers and more challenges to understand all aspects related to risk management.

Key findings are presented in the Table 3 below.

Table 3. Review of past studies on the topic

The table presents a list of studies published between 2010 and 2025, together with their main results.

Article	Scope	Key points
Khinvasara et al. (2023): Risk Management in Medical Device Industry	Review of general risk management process in medical device industry	Risk management is mainly based on technical risks (such as errors in use) and for example business risks are not given much attention. The implementation of risk management is considered to be generally difficult because the risk management process should have a strong connection to other processes.
Kortelainen et al. (2025): The role of ISO 9001 and ISO 13485 Quality Management System as drivers behind health technology supply chain performance and evolution	Integration of ISO 13485 with supply chain	Different standards tend to evolute and form combinations with other relevant standards and processes.

Article	Scope	Key points
Karnika et al. (2020): Medical device risk management	Risk management process explained according to ISO 14971.	The focus of the study is mainly in general risk management process. The study does not cover how risk management process should be linked to other company processes and the view is limited mainly to single process.
Javanmardia et al. (2024): Exploring business models for managing uncertainty in healthcare, medical devices, and biotechnology industries	Risks related to companies who develop medical devices – a research study	The research paper is about medical industry related risks relating to company business. Research is a literary study of 34 recent research papers. Also “product-service system business model” (similar to SaaS) is included. Regulatory related risks produce uncertainty to medical device companies in addition to other sources of uncertainty.
In (2021): Cybersecurity: Risk management framework and investment cost analysis	Cybersecurity: Risk management framework and investment cost analysis	Focus on cybersecurity issues. A separate cybersecurity risk management model is introduced. Also, human role in cybersecurity is briefly mentioned and included in cybersecurity risk management model.
Mahamudur (2022): Electrical and mechanical troubleshooting in medical and diagnostics device manufacturing: A systematic review of industry safety and performance protocols	Reporting of hazards related to electro-mechanical issues, a literature review.	The varying format of reporting hazards might require more standardized and harmonized ways of reporting.
Kivimäki (2021): Development and implementation of a quality system for in vitro diagnostic medical software	Company interview related to the implementation of ISO 13485 and ISO 14971 for medical software products	Documentation requirements seemed to require lots of work.

According to previous research studies related to risk management, there has been a need for harmonized ways of reporting risks, including business risks to risk management processes and the need for heavy documentation was noticed. Since the companies have very different products, different products may require different ways of risk management. Different ways typically produce very different documentation, and companies may have difficulties to fully understand the requirements of regulation.

Risk management of medical devices follows typically the traditional do-plan-check-act -cycle where risks are systematically collected, mitigated and the effectiveness of the risk management process is observed (Khinvasara et al. 2023). In medical devices, risk management should not be just an isolated process. Instead of being an isolated process, risk management should be seen as a

cross-functional process with interconnections to other processes. Since this kind of deep integration requires more knowledge and maybe also mor involvement, this kind of holistic approach may often seem hard to implement. Also Master thesis from Kortelainen and Milovanov discuss about the intersection of ISO 13485 with supply chain management and integrating ISO 13485 to supply chain management (Kortelainen et al. 2025).

Other research papers also concentrate on risk management process only and other processes in the medical device development are not addressed in the study (Karnika et al. 2020). This kind of approach may be difficult when all product development and support processes should concentrate on identifying and reducing risks.

Healthcare industry has typically many kinds of risks. In addition to product risks of the medical product, companies tend to have a wide range of various types of risks (Javanmardia et al. 2024). ISO 14971 standard is often implemented in a way which manages mainly product risks. Also, business risks, especially if subcontracting is used, may produce product-related risks which may affect product safety. This narrow view may be the result of isolated risk management process.

Cybersecurity risks may also affect the safety of SaaS-type medical products. In other research papers, a separate process for managing cybersecurity risks is introduced. Also, the human role in cybersecurity risk management is briefly mentioned (In 2021). Since the product risks of the medical product may contain also cybersecurity related risks, adding the cybersecurity viewpoint to risk management might improve the process. Especially SaaS-type of medical devices could benefit from improved mapping and mitigation of cybersecurity risks.

A research paper from Mahamudur reviewed 82 peer-reviewed articles related to mechanical and electronical -related hazards and risks of medical products. As a result, one of the biggest problems in risk management and incident reporting were related to various forms of hazard reporting and more unified and harmonized ways of hazard reporting would be needed (Mahamudur 2022). Although the reviewed study was not from medical software devices, the results indicate that certain systematic ways of reporting risks and hazards is important for risk management and risk mitigation. Risks reported by manufacturers are also used in post-market surveillance analysis and more harmonized guidelines and instructions might enhance the utilization of risk related information.

Iina Kivimäki has conducted a study related to development and implementation of quality system for medical software devices (in-vitro). The study included semi-structured interviews with six

companies including literature search. The study concentrated on agile software development practices and implementing the quality management system including risk management. According to interview, documentation requirements for ISO 13485 were seen to be requiring lots of work. Risk management activities were also integrated to software development processes and various tools (like Excel and different Atlassian plug-in -software) were used (Kivimäki 2021). Since many medical software products may have been started to produce long before EU medical regulation, the lack of proper documentation might be also a problem when the implementation of the quality management system and risk management processes is taken into use. Also, the role of automatic generation of required documentation seems to be wanted functionality.

2.10 Conclusion of possible trends derived from recent studies

The summary and possible trends derived from previous studies are:

- Risk management in medical devices is rather difficult and there is a risk that the risk management process will become single, isolated process.
- Instead of being single, isolated and product risk-centered process, also other company-related risks should be considered
- Current ISO 14971 may not contain sufficient cybersecurity risk -related viewpoint and there might be some improvement needed for cybersecurity risks

2.11 ISO 14971 convergence with EU AI Act and ISO 42001

One very important viewpoint can be derived from EU regulatory. Since EU has published AI Act, the possibly increase in AI usage (for example, Sitra 2026) may increase the need for advanced risk management in AI applications. For example, Nordea is planning to utilize AI for processing of sensitive financial data (Nordea 2026). Since ISO 14971 presents an industrial standard for risk management in highly regulated and most safety critical medical world, ISO 14971 practices may also need to be implemented outside medical device industry. This need has already acknowledged in AAMI TIR34971:2023 -standard where ISO 14971 risk management methods are used in artificial intelligence applications (AAMI Array 2023). There is also a standard ISO 42001 for the safe use of artificial intelligence (ISO 2023).

Regulatory related to medical devices are under constant changes and similar fast changes can be also seen in the development of artificial intelligence. Medical device risk management standard is

based on minimizing the patient risk and regulatory takes account of lifecycle management of medical software products. Because of those similarities to artificial intelligence applications, one possibly outcome from applying EU AI Act may lead to implementing medical device risk management standard to AI applications processing sensitive data, such as financial data.

At the moment, there has been some discussion related to implement ISO 14971 also to general AI applications processing sensitive data (Hardian Health 2026, AAMI Array 2024, MPO Magazine 2025). Extending to use of ISO 14971 to AI applications will also reduce the number of multiple risk management standards. As from a personnel point of view, it might be also easier to find suitable workforce with previous experience related to risk management if the same risk management standard is applied in different industries.

3 Research question and methodology

The main research question of this thesis is about identifying current trends related to the risk management of SaaS-type of medical product. The risk management plays a key role in medical software development, operation and general company processes. Poorly developed risk management process may also have an effect to patient safety, company reputation and financial issues and cause various problems. Since it is typically easier to plan and implement risk management actions in very early state of software product development, knowing about emerging risk management trends is beneficial for proactive risk management. Because of technical development, especially complex software -based medical devices are difficult from the risk management point of view. Estimating possible future trends may ease the risk management process implementation. Identifying also required more general guessing-type of approach which will suit better to this thesis when compared to more scientific methods.

The SaaS-type of medical software product was selected because of cybersecurity point of view. The study is limited to mainly to EU area issues to limit the results. Other studies may be needed to cover other geographical areas with various national regulation. Since there can be issues which are related also to non-medical software products and issues outside EU, these issues will be discussed if these are relevant according to research subject.

The study is risk management -based because the EU medical regulation aims for reducing patient risks. Risk management -view is concentrated on patient risks and risks which are interconnected with patient risks.

3.1 Research question

This master thesis is about researching possible emerging future trends related to implementing ISO 14971:2019 to the Software as a Service (SaaS) -type of medical product. The main research question is:

- what are the current trends – including opportunities and risk -related to implementing ISO 14971 based risk management for SaaS-type of medical software
    - current status and trends will be searched mainly from EU regulation and research papers related to risk management of medical software product

The research question is limited to ISO 13485:2016 and ISO 14971:2019 and to SaaS-type of medical software products in EU area (ISO 2016, ISO 2019). According to EU regulation, a quality management system must be used when developing a medical product. A medical product can be a physical product, algorithm or other software product. ISO 13485:2016 requires that risks related to medical software product must be addressed by using relevant methodology. The relevant methodology is in this case, the use of ISO 14971:2019 risk management standard which is a risk management standard especially for medical devices.

Figure 4 below illustrates the planned research for mapping future trends. Research papers, including relevant EU regulations, are analysed and synthesis will be done for mapping possible future trends.

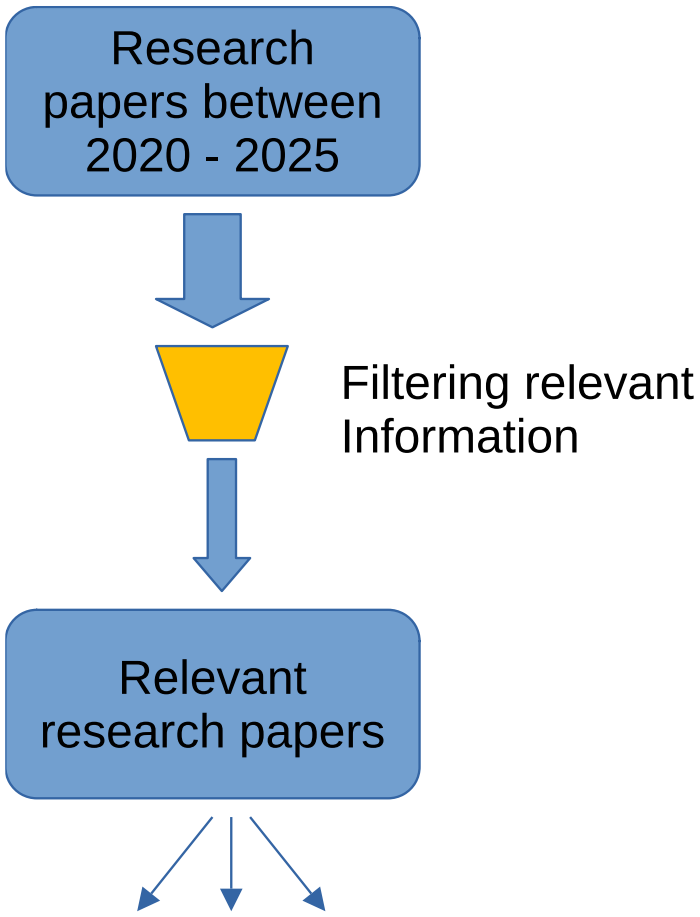

Figure 4. The general idea of this thesis for mapping possible future trends.

The risk management is the key issue for developing medical devices and therefore the study is done from the viewpoint of risk management. Because of variety of both physical and software

medical product, the study is done from the viewpoint of Software-as-a-Service -type of software medical products.

The form of this thesis is divided as follows:

- general review of risk management studies related to medical products
- more specific view of ISO 14971 implementation in SaaS-type of medical products according to current EU regulation and research papers
    - Analysis of regulation and especially research literature data
    - Synthesis of collected information for mapping possible future trends

Main source of information to be used is Google Scholar and research papers between 2020 – 2025. The division between general review of risk management issues and specific view of ISO 14971 implementation was done by the author. Also filtering irrelevant research papers was done by the author.

After reviewing relevant research papers, possible future trends related to implementing ISO 14971 risk management standard to SaaS-type of medical product were estimated from the results.

Reviewed research papers will be then divided into subgroups which will present trend. Finally, the trend will be visualized and explained. As a result, the general future trends and their significance can be roughly defined. Found trends will be categorized to rough categories where possible rough future risk management trends will be identified. Research papers will be limited to such research papers which relevant to SaaS-type of medical device.

Research papers were selected to research materials because possible future trends might be visible in research studies at the first place. Other sources were also considered but rejected because certain reasons. Those other sources considered and rejection reasons were:

- Global databases for risk reporting sources (HPRA 2026, ANSM 2026, BfArM 2026, Swissmedic 2026,MHRA 2026) do contain risk reporting information but because of various formats of risk descriptions, various medical product types and product specific - information, the amount of manual work would be heavy and risks would be most likely related to some random product problems instead of bigger picture

- News related to risks were also considered but typically newspapers do not have very good understanding of medical software risks and typically only major occurred risks will end up in newspapers

- Interviews of company representatives were also considered but since risk management is typically company confidential material, probably the interview results would be more or less limited. Also risk management personnel knowledge related to future trends may be inadequate.

3.2 Research methodology

This research is quality based research where the contents of selected research papers will be reviewed systematically (Salminen 2023). The reviewing is done by the author, and possible trends will be extracted according to the main conclusions of reviewed research papers. Systematic approach allows extracting relevant information from a specific research topic, and this approach will provide the most relevant information from the research question. Since there are no statistical calculations done, the only meta-information will be simple visualization of the most common findings. The research method will collect information from previous research papers and the the information will be integrated and synthesized in orderd to gain new knowledge.

This research does not include collection of the original data since the original data was already collected by authors of research papers. Therefore, no ethical pre-assessment is not needed. All reviewed materials will be listed and research will be documented. A good scientific practice is used (TENK 2023).

3.3 Data collection

Research papers were collected with a following criterion:

- Google Scholar was used, research papers were searched from the last five years

- Keyword ISO 14971 was used and combination of keywords of MDR, ISO 14971, ISO 16485, risk management, software

- 20 the most relevant papers will be reviewed; the relevance will since there are over 3000 research papers from various topics, selection is done manually

    - manual selection is done by reflecting the contents of research papers to regulation, standards and thesis research question
    - reviewing was done by reading the research paper
    - if there are future trends, it was assumed that very rough guidelines for future trends will be visible in reviewing 20 relevant and recent research papers
- key points from those will be identified and it is assumed that the most common key points may predict possible emerging future trend

3.4 Classifying possible future trend from literature review

When the research papers are reviewed, key findings from research papers will be roughly classified to relevant main scope of possible future trend. This classification may assist detecting possible future trends by making rough classification. The exact contents of the trends will be textual descriptions related to these pre-defined categories.

Since there are not any information about real future trends, it was estimated that there could be four main scopes. The use of these predefined scopes may help to very roughly classify possible risk management trends and to give some rough guidelines related to implementing ISO 14971 risk management to SaaS-type of medical software product.

Combining findings and rough scope of findings, the possible future trend can be retrieved.

Scope has been divided roughly to certain groups which are

- General (general trend)
    - The trend is related to general implementation of ISO 14971 in SaaS-type of software development. The research paper may contain general viewpoints to implementing standards, software development issues or other similar issues
- Cybersecurity (risk management trend is related to cybersecurity)
    - Reviewed research paper was mainly related especially cybersecurity risks or issues related to cybersecurity
- AI (trend is related to AI)
    - Research papers related to AI or AI's role in implementing ISO 14971 in SaaS-type of medical software device development
- Human (trend is related to human-centric issues)

- Research papers which enhanced human role in implementing ISO 14971 or which were related to human-factors in medical software development

Research papers will be reviewed, and key points will be extracted according to key points of each research paper. Key points will be viewed from the point of view of the research question of this study.

Possible future trends are derived from the reviewed research article. Trends are generated by examining key points of research article and then defining possible trend. The trend definition is done by the author according to the context of the research question.

Since the future trend extraction is based on author's assumptions, it is important that there is a clear linking between research papers and exact future trend. If the trend estimation is done by other person, clear linking will help reproducing or expanding the results.

3.5 Limitations of the research

This research is limited to certain number of research papers from specific source (Google Scholar). Since the selection is done manually, it is possible that some key findings might be missing or the conclusions may suffer from the small number of reviewed research papers. However, using the automated tools for analysing and retrieving research papers may also present a problem since the automation might not fully understand the context of research papers in this study. Therefore, manual approach was used for selecting research papers.

3.6 The role of AI in this thesis work

AI tools were not used in this thesis because not all AI tools can access research papers in Google Scholar. Although AI tools are effective for retrieving information, the main problem with AI tools is the classification of found documents. Classification of research papers and other documents require the understanding of the role of the document in the context of this study. AI tools, like Gemini AI and Microsoft Copilot are not very familiar with the actual medical software issues and typically different query results mixed relevant and irrelevant contents and sometimes missed the key points or the big picture was not clear.

These problems with AI and other automated analysing tools may also reflect the complexity of applying medical regulation and risk management issues. Since the environment is very complex, typically human is needed for making the final decisions and analysing the relevance of results.

3.7 The result of literature search for planned trend study

As a result of research papers search, there were thousands (almost 4000 research papers totally in Google Scholar's search results between 2020-2025/2026, depending on the use of keywords used). Research results were reviewed and relevant research papers were selected. Reviewing required manual checking of research paper contents.

As a result of literature search, 20 relevant research papers were selected. Selection criterion was as follows:

- Was the research paper published at least five years ago?
- Is the viewpoint closely related to implementing ISO 14971 to especially SaaS-type of medical software product?
- Are the research viewpoint in line with EU regulations and possible other standards. Regulation is considered to be following guidelines of possible future trends and regulation will set guidelines for practical implementation.
- Does a selected research paper give some kind of practical problem and can trend be derived from conclusions of specific research papers
- Finally, similarities between conclusions (possible emerging future trends) will be identified and data will be synthesized in order to define major future trends

3.8 The discussion related to literature search for planned trend study

Some research papers did not addressed SaaS-type of medical products and some contained only too general discussion about general problems in risk management. If the research paper viewpoint was limited to single, very specific problem (like the risk management in specific single medical facility in specific geographic location), that research paper was left out from this study since the aim of this study was to find more general development paths.

Since there were thousands of research papers related to somehow to the subject, it was estimated the search engine will list the most relevant related to keywords used. After each search, search results were manually reviewed until there seemed to be no longer relevant search results (search results did not no longer produce any relevant information after reviewing tens of results).

Automated retrieval and analysis could have speeded up the process. However, there is a risk that more results will bring more unwanted “noise” (research papers falling outside thesis’ research question) and therefore the use of automatization may not bring enough help defining general future trends.

It was noticed that there had been also some studies which addressed the current state of implementing ISO 14971 and the methodology in those research papers followed the methodology used in this thesis. The aim of this thesis was to give future prediction of trends related to current situation and those earlier research papers were used as a groundwork for this study.

4 Results

This chapter will go through the relevant regulation and guidance and findings of literature search results. Relevant research papers will be analyzed from the point of view of the research question. Possible future trends will be extracted. EU regulation and guidance represent the current implementation of medical software risk management issues and therefore it is very important to understand regulatory and guidance related issues before research paper review.

4.1 EU regulation and guidance

If the software fulfills the definition of a medical product, the software must also fulfill the regulation related to medical products. EU has published various laws and guidance related to medical products. The manufacturer must be aware of those and understanding the regulation also helps understanding the increased role of risk management. The whole EU medical regulation aims to reduce possible patient risks. Since there are many kinds of medical software products, EU has also published additional guidance documents to clarify issues which may be unclear or were not defined earlier.

The table 4 below presents selection of recent guidance related to medical device regulation. Selection was done by listing relevant guidance documents published between 2020 – 2025 by EU. Regulation relevant from the risk management point of view was listed. If EU does not have updated regulations, regulations from other medical authorities were listed. The list is not meant to be complete but to give a general overview of the development of medical device regulation from the risk management point of view.

Table 4. Review of recent guidance related to medical device regulation

Guidance document	**Contents and publication date**	**Issued by and risk related purpose**
General Principles of Software Validation; Final Guidance for Industry and FDA Staff	Software validation guidelines for validation for especially cloud-based software / September 24, 2025	FDA (U.S. Department of Health and Human Services Food and Drug Administration): for addressing the use of software for product development purposes and better validation for especially cloud-based software (earlier corresponding guidance was mainly for on-site software validation). ISO 13485 standard requires validation of software tools used in production of medical software. Also the produced

Guidance document	Contents and publication date	Issued by and risk related purpose
		software itself must be validated so that the software will meet requirements of the end users
MDCG 2023-3 rev.1 - Questions and Answers on vigilance terms and concepts as outlined in the Regulation (EU) 2017/745 under Regulation (EU) 2017/746 - November 2024	Revised instructions related to reporting serious incidents for medical devices / January 7, 2025	EU, Directorate-General for Health and Food Safety / Risk management is very complex issue, and the guidance defines some questions especially related to reporting from serious incidents. Reporting risks is important because there is a centralized need for collecting risks from various medical products. These reported risks can be used between manufacturers to spread information about risks and making risk reduction more efficient. Risk management process includes also post-market surveillance report which is typically done annually. One part of the post market surveillance report is to study vigilance reports and risks reported by other manufacturers.
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)	Rules for applying artificial intelligence (AI) for medical devices / June 13, 2024	The European Parliament and The Council of The European Union / The usage of artificial intelligence and the mitigation of risks related to that explained. EU does not ban the use of AI but these rules will give instructions and guidelines how AI can be utilized in medical software products. From a risk point of view, AI can be also used for other purposes like scanning and monitoring cloud environment from different threats.
Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices (September 2023)	More precise instructions for defining what is the medical device, also some practical examples are included / September 27, 2023	Directorate-General for Health and Food Safety / Definition of the medical device is explained more clearly with relevant examples. Since the quality system (ISO 13485) is risk based, it is essential to identify when the software is a medical device which requires fulfilling the EU medical regulation. Because of fast technology development, there is a need to clarify and give practical examples which products are classified as a medical product.
Add 1 - MDCG Position Paper on the application of Art.97 MDR to legacy devices for which the MDD or AIMDD certificate expires before the issuance of a MDR certificate	Instructions for old (legacy) medical devices for meeting the regulatory requirements / June 30, 2023	EU, Directorate-General for Health and Food Safety / The development of old (legacy) was typically done before the medical regulation and this guidance defines how to apply regulation issues for such legacy devices. Since old medical products

Guidance document	**Contents and publication date**	**Issued by and risk related purpose**
		have been developed without knowing EU medical regulation, those products may not be documented well enough. The risk management issues may not have been implemented and integrated according to the latest regulation. The transition from old medical device development towards regulated development, is described in this document.
Update - MDCG 2020-16 Rev.2 - Guidance on Classification Rules for in vitro Diagnostic Medical Devices under Regulation (EU) 2017/746 - February 2023	Medical device classification rules explained / February 10, 2023	EU, Directorate-General for Health and Food Safety / medical device risk class classifications explained. EU medical device regulation is heavily based on device risk class. Reporting and actions needed are based on risk class and typically products with higher risks must be addressed more carefully. Since there are many kinds of software products, defining the appropriate risk class in the same way in different circumstances requires clear guidance.
Application of Regulation on Medical Devices – EU rules to ensure safety of medical devices	An example of news promoting the safety of medical products and general mitigation of risks related to those / May 26, 2021	EU, Directorate-General for Health and Food Safety / Typical general news where the safety and risk management issues are promoted. Since technology, software production methods and other similar issues develop fast, EU frequently publishes information about coming changes, notifications related to deadlines and other relevant information. From risk management point of view, following of that information is vital for keeping processes – including the risk management process – up-to-date and making sure, that all EU guidance documents will be read and possible changes will be implemented.
Covid-19: Commission Notice on audits to be performed by notified bodies	Safety guidelines for performing audits during the time of Covid-19 instructed / January 11, 2021	EU, Directorate-General for Health and Food Safety / Audits (also related for auditing risk management issues) performed during Covid-19 explained. This is an example of how risk management process can react to changing circumstances. Since the quality management system will be audited in order to ensure that EU medical regulation is met, there might be a situation – like Covid pandemic – which may cause situation which requires new instructions. Therefore EU published safety guidelines

Guidance document	Contents and publication date	Issued by and risk related purpose
		related to mitigating risks related to pandemic issues.

From the risk management point of view, regulation itself had moved towards unspecific definitions towards more modern and up-to-date regulation. The regulation aims for mitigation of risks related to medical devices and since the environment and devices are under constant change, regulation requires constant updating.

Since the software development tools of medical software products need to be validated before being taken into use, FDA has published a new instruction which describes especially the validation of cloud-based software development tools (FDA 2025). Earlier, software development tools were more on-site tools which were installed on personal computers. The new instructions are more suitable for modern IT environments. Since EU has no such validation guideline document for validating, especially cloud-based software, it might be logical if EU will publish similar guidance soon.

Because of increased complexity and unclear risk incident reporting, EU has published instructions related to reporting risk incidents to authorities (EU 2025b). Since the complexity of medical software and especially SaaS-type of medical software have increased, revised and more specific instructions are needed. Risk reporting and collecting incidents by authorities will be used for improving the general safety of medical devices.

Because of the increased use of artificial intelligence, EU has published a law related to the safe use of artificial intelligence in medical devices. The use of artificial intelligence is not prohibited but the possible risks must be known and to be mitigated. AI law also describes the forbidden usage of AI in the field of medical devices and an example of forbidden use of AI is to use AI for manipulation and social ranking of patients. AI law will be taken into use in 2026 (EU 2024a). The increased usage of AI had created the need for understanding the role of AI in medical devices. AI can be used for analyzing medical data, but it must be known what the exact use cases for AI are. Since AI is constantly developing, it might be possible that EU will publish later more specific AI related guidance which will include more use cases.

The definition of what is a medical device and what is not was earlier a bit unclear. Therefore, EU had published a borderline manual which defines boundaries for definitions related to what kind of product is a medical device and when the device is not classified as a medical device (EU 2023a).

This is especially important for SaaS-type of medical devices since software products can consist of many different functionalities. Software can be used for storing and transmitting medical data and according to borderline manual and regulations in general, the plain storage feature is not considered as a medical product. However, if the medical data is modified with some kind of algorithm, according to borderline manual, this kind of software is considered as a medical device. Earlier this definition was not clear since there was no official definition where the border exactly goes. The borderline manual also discusses non-software medical products and defines borders between medical and non-medical products.

Since medical related regulation has emerged and evolved in recent years, there are some medical software products whose development had begun before the regulation was known. Therefore, software development and risk management may have been done long time before the regulation. After the regulation, there may be gaps in medical software documentation and processes, and therefore EU has published instructions how to apply regulation to such medical products (those are called “legacy” products) whose development have begun before regulation (EU 2023b). For SaaS-type of medical software, it may have been common that the software had been first on-site software which was installed to personal computers. When cloud-based architecture appeared, the software may have been transferred to the cloud-based version where users can use the software via browser. Cloud-based transitions may have also affected the business logic of software producers causing transition of business logic from selling products to selling services. Also, earlier risk management issues may not have been enough after transition from on-site to cloud based and therefore new specific instructions for legacy devices are needed.

The EU regulation requires that medical devices must be classified. The classification is based on the possible risk to the patient. Since regulation and standards are risk-based, the classification also affects the level of risk management measures. Because of the complexity of medical devices, EU had published a guidance how risk classification must be done for medical devices and what issues affect risk classification (EU 2023c). Risk classification affects also to time schedule for making medical devices compatible with medical regulations.

The European Union has been active in informing and promoting the safety of medical devices and therefore several guidelines, news and safety related guidance have been published (EU 2021a). Since the medical device regulation is rather heavy to implement to companies, the management of information related to regulations and for promoting the risk management issues is vital for medical device regulation.

Regulations also apply to the risk management process relating to auditing of the quality management system. This is used for ensuring also the safety issues related to people working with the risk management of medical software (EU 2021b). The risk management issues are not related only to technical issues but also affect human related issues. EU regulation is more based on technical viewpoints of risk management and there is no specific guidance related especially to human factor issues. Since the EU regulation will continue to cover risk management issues more extensively, it might be likely that such guidance will be published.

4.1.1 Summary of findings from medical device regulatory

As a conclusion of findings from reviewing medical device regulatory issues, certain issues have arisen:

- Medical device risk classification and the medical device classification itself typically require some expert work since SaaS medical software can be very complex and there is a clear need to define borders for regulations
- The use of AI has brought a whole new viewpoint to the development of medical devices and for risk management of medical devices
- EU regulations are increasing, and this will most likely have an effect to the workload and training needs for quality personnel working with medical device related issues
- The development of technologies used for medical devices (like cloud-based software development tools) requires new guidance and possibly also new definitions related to regulatory borders
- Currently EU regulation related to risk management of medical products is more technical and there might be a need for defining also non-technical, human-centric issues and methodologies related to risk management

4.2 Review of relevant research

This chapter will review 20 relevant research papers. After reviewing, key findings will be extracted and possible future trends will be defined.

A research paper from Kiki Yang underlined the importance of integrating ISO 14971 into ISO 13485 and other similar standards. Research paper also highlight the importance of integrating risk

management process with other product development and quality management processes (Yang 2024). Since many standards may contain similar functionalities and requirements, it would make sense that those similarities might become integrated into one standard. The concern about isolated risk management process and the possibly need of better integration of risk management process were also discussed in earlier research papers (Javanmardia et al. 2024, Khinvasara et al. 2023, Karnika et al. 2020). Instead of having separate risk management process for cybersecurity risks, business risks and human-centered risks, maybe it could be relevant to combine all those into update version of ISO 14971. The integration would be a logical continuum for evolution of ISO 14971 and the increased importance of cybersecurity in SaaS-based medical device. Regulation inside EU is often criticised (for example Yle 2025c) for heavy burden of regulatory issues which may also cause financial burden and slow down the development of medical devices.

Possible emerging trend derived from the reviewed research paper:

- Increased integration of ISO 14971 into other relevant standards

Research paper from Stephen G Odaibo presents a framework of risk management of incremental development of medical software and implementing requirements from ISO 14971 (Odaibo 2021). Typically, SaaS-type of medical software or medical software in general is developed by incremental steps. A new functionality is added, or existing functionality is modified. Each modification may alter the functionality of the medical product and therefore there is also a possibility that new risks will appear, or existing risk mitigations will be broken. Since there had been a need for EU to clarify the definition of the medical product (for example EU 2023a), the complexity of the software may present changes for software development. When artificial intelligence is used as a part of the software, possible changes to software functionality may be even more difficult to identify.

Possible emerging trend derived from the reviewed research paper:

- Managing software changes in incremental software development of SaaS-type of medical product will require more attention when software becomes more complicated

According to Master's thesis by Markus Ojanen focused in observing challenges related to implementing ISO 13485 standard in medical device production. According to the study, it was often found difficult to interpret and implement standard requirements. It was also observed that the implementation of ISO 13485 required creation of various definitions which are needed when measuring the effectiveness of the standard implementation. Identified future trends consisted of

increased communication between medical device producer and end-users and possible evolution of standard to integrate better to the modern software development and integration to other standards (Ojanen 2024). Especially SaaS-type of medical software product is used by different customers, the role of feedback and collecting the feedback may play bigger role in the future. It was also noticed that when the complexity of the software product is increased and especially when artificial intelligence is taken into use, the implementation of the standard may get more complicated. On the other hand, after the basic framework of ISO 13485 and ISO 14971 is implemented and the knowledge is increased, it may be easier to implement the new versions of standards. Collection and reaction to feedback of users is already required in ISO 13485 but in SaaS-type of medical software product, there might be various kinds of users. The increased number of different users may require enhanced collection and utilization of user feedback.

Possible emerging trend derived from the reviewed research paper:

- The increasing complexity of SaaS-type of software product may lead to need for enhancing collection of user feedback for risk management purposes

In a research paper concentrating on syringe manufacturing and emphasizes on regular and systematic checking of ingredients. The focus of ISO 14971 risk management is in documenting components relating to manufacturing of syringe, identifying main risks and implementation of risk mitigation actions (Sharma et al. 2024). For a software product, such approach is also effective and when the risks are identified and the whole software development process is under constant observation, it is easier to define and mitigate possible risks. Since the complexity of medical software and medical software development tend to be increased, the importance of managing information may play also a big role in the future.

Possible emerging trend derived from the reviewed research paper:

- The importance of identifying software components and mapping risks will remain important issue in the future.

According to research conducted by Ajax Raymond, medical software applications operating in networks require additional risk management actions. Cybersecurity issues must be considered in a design phase. The software products must be tested with penetration tests. When the medical software is in use, continuous monitoring must be performed to track possible threats and security violations. Also, AI and other sophisticated tools can be used for monitoring the safety of cloud

software. The research also defines possible future trends related especially to future cybersecurity mitigations and those trends are (Ajax 2025):

- digital twin simulations,
- global regulatory harmonization,
- patient-centric security approaches
- underscoring the need for proactive collaboration between manufacturers, regulators and healthcare providers

Since ISO 14971 is mainly an ordinary risk management standard for medical devices and cybersecurity issues are dealt in a separate standard ISO 27001 (ISO 2022), there might be a need of aligning of those standards and applying cybersecurity issues also to medical safety related issues. According to research by Ajax Raymond, the use of SaaS-type of medical software has increased the need of better collaboration between different stakeholders relating to safe operating in networks. When combining ISO 14971 risk management approach with ISO 27001 standard, there are no clear instructions how this collaboration can be done safely and what is required. Similar results were also discussed in a research paper of Carmichael et al. related to identifying possible cybersecurity risks in very early stage of development (Carmichael et al. 2025). The benefit from identifying possible risks in very early stage of product development will be much more cost-efficient than fixing possible problems after the final product had been launched.

Possible emerging trend derived from the reviewed research paper:

- Cybersecurity brings the need of alignment of cybersecurity risk management with medical software risk management and expanding the scope of risk management actions

A research paper has studied the consistency of IEC/ISO standards on safety and quality related to applications of telehealth and mobile applications. Analysis was divided into three subdivision: quality and safety management, core healthcare process and resources. The study is focused on how different safety and quality standards are aligned together. According to the study, there are some mismatches in alignment and without applying ISO 14971, patient safety may be compromised (Meijer et al. 2021). Standard IEC 62304 is a software lifecycle standard which is traditionally used in software development. The standard suggests that the software is divided into software units which will be integrated into system (ISO 2006). Since ISO 14971 is stricter related to managing risks and patient safety issues, applying only IEC 62304 may not provide enough patient safety.

Also, if IEC 62304 is applied, there are some risk management parts in both standards – IEC 62304 and ISO 14971 – but those parts do not fully align together. The use of separate standards may then lead to the situation, in that there would be a need for some kind of upper-level control.

Possible emerging trend derived from the reviewed research paper:

- Since there are many standards related to patient safety, there is a need for some kind of upper level control for ensuring better alignment of different standards

According to the article Regulatory Prospective on Software as a Medical Device, especially cybersecurity issues, decommissioning (end-use management), safety issues and high costs of the medical device and the difficultness of managing complex design and development process were seen problematic. Since there are different standards and regulations used in different parts of the world, managing the global regulatory issues were seen difficult (Foram et al. 2022). Since the software development methods and tools typically change after time and new ways to implement medical device software will appear, this causes pressure to regulation to be up to date with current implementations. If the definitions are different worldwide, ensuring the global regulatory compliance would most likely be needed for global regulatory standards.

Possible emerging trend derived from the reviewed research paper:

- Instead of national and regional medical device regulatory standards, the use of general global standards and regulations would be better for medical software intended for global markets

There is medical software which can be developed in-house and which will fulfill the definition of medical device and which will be used in medical care. This kind of software is also regulated and must fill the medical regulation. According to the study by Lagerburg at al, an existing software development process must be transformed so that the medical regulation needs are met. One part of transformation towards regulatory compliance is implementing the risk management system. According to the study, currently there are no regulatory guidance documents or information on how those in-house products will be translated into regulatory compliance. In that research study, the software development process was splitted into smaller parts, regulatory related issues were added and responsibilities were defined. As a result, the in-house software production process becomes regulatory compliant (Lagerburg et al 2025). There is one EU guidance document related especially to in-house software (EU 2023d) but probably more guidance is needed.

Possible emerging trend derived from the reviewed research paper:

- In addition to legacy medical software products, there is a need for similar guidance document for in-house developed medical software

Beckers has studied how EU medical regulation affects medical software using AI and how a regulatory roadmap can be set to software medical products. According to research study, one problem is that if AI tools are developed in-house and the main purpose of the medical software is very narrow, there might be very little relevant guidance from the regulation and company must have experts understanding both the software related usage and regulatory issues (Beckers et al. 2021). This kind of development trend might increase the requirements for people working with medical software products. Since the regulations are constantly changing and improving, the need for qualified personnel might be an important issue for companies.

Possible emerging trend derived from the reviewed research paper:

- Because of fast technology development and evolving medical regulation, requirements for qualified product development personnel will increase in the future

According to the doctoral thesis of Kheir Omar, meeting regulatory compliance is typically harder to start-up companies which may typically have a very specific and unique medical software product. Especially medical software start-up companies have problems related to the lack of market Fitness of the developed product, absence of funding and improper management. Typically risk management process is concentrated on technical risks of the product and typically less attention is paid to usability and process risks. The thesis also pointed out that especially Small start-up companies may suffer the lack of management involvement (Kheir 2023). Although this references doctoral thesis did not present any silver bullet for successful risk management of medical software, the thesis highlighted the fact that managing risks requires high integration of the risk management process and company management involvement for supporting the maintenance of the quality management system and risk management process.

Possible emerging trend derived from the reviewed research paper:

- In order to succeed, all company personnel must be highly involved to the applying and integration of the risk management process

According to research by Niamh Nolan and Olivia McDermott, Failure Mode Effect Analysis (FMEA) is the most common used tool in risk management. FMEA concentrates on defining

possible failures and failure causes including risk reduction. As a result, risks will be identified and risk probabilities and severities will be estimated. According to this research study, the repeatability and difficultness of applying risk management process to subcontractors were seen problematic. The research study suggests that also other risk management methods (like the use of hazard analysis) should be used in accordance with FMEA. Also, the complexity of risk management and the lack of personnel training was seen as a problem (Nolan et al. 2024). This research study highlights the fact that understanding the risk management process and making personnel aware of risk management issues are important part of medical software development. Very similar issues and future trends were seen in previous research by Kheir Omar (Kheir 2023).

A research study conducted by Han Shihui et al. was about comparing different standard requirements (ISO/IEC 25010:2011) to medical device related standards (ISO 13495 and 14971). Research study found similarities between those standards and the mapping of similar functionalities between standards were possible (Han et al. 2020). Since there are many medical software device related standards, the use of some kind of framework for mapping different standard requirements into one framework could possibly reduce the documentation and implementation burden related to regulatory. Different standards have different viewpoints to product development and availability of one single framework could help combining different standards. A bit similar idea was discussed in other research study by Meijer (Meijer 2021).

Master's thesis of Mika Peltokorpi contains a study related to resilient risk management of medical devices. The idea of thesis was to conduct interviews related to processing times of detected risks in product development. According to thesis, the use of visualizations and standard risk report templates helped product development organizations to react more rapidly to detected risks (Peltokorpi 2023). Since software development is moving towards increased automation, perhaps automation could also be applied to risk management tasks. Visualization, risk report templates and use of different automated reports could help managing risks. Automatic reporting could also help with increased medical regulation. The increased level of automation is also discussed in the study conducted by Häppölä (Häppölä 2024). According to Häppölä, automated tests related to testing of the medical software can generate also automatic verification evidence (related to fullfilling the requirements of the medical regulation automatically) but human approval is still needed for approving the automatically generated verification results. Also research paper from Svempe identified that gathering clinical evidence related to medical products will require lots of resources especially from smaller companies and causing possible delays for smaller companies to get their

products in the market (Svempe 2024). The complex and extensive medical regulation requirements may therefore require solutions; either simplifying the regulation or more automation.

Possible emerging trend derived from the reviewed research paper:

- The software development moves towards higher levels of automatization and automatic creation of regulatory requirements

A research project conducted by VTT researched for best practices for transition to the medial device regulation, artificial intelligence compliant RegOps models and other medical software development related to healthcare. The project made co-operation with six industrial partners who were related to the production of medical software devices. According to the study, the use of artificial intelligence tools is difficult from the viewpoint of regulation (EU AI act was published years after this study) and implementing the regulatory related requirements were considered difficult and time consuming. Co-operation with other similar companies and exchanging experiences were beneficial. Regulation requirements were integrated into workflows of companies to meet regulatory requirements (Lähteenmäki et al. 2023). Since software development is moving towards higher automation, the need for automation in regulatory work was a key element in this study also. Also, earlier study by Peltokorpi had similar views (Peltokorpi 2023).

According to Ph.D Dissertation of Svana Helen Björnsdóttir, there is a gap between academic risk management research and practical implementation of risk management in medical devices. According to this study, different risk management activities defined in different standards lack uniformity related to terminology and guidance. Also risk management could be better if state of the art -tools were used. Ph.D dissertation proposes new models for enhancing risk management methods proposed by current standards (Björnsdóttir 2024). Similar view related to the need of some kind of upper-level control of medical device related standards and risk management issues were also presented in previous research papers (Meijer 2021 and Han et al. 2020). Since medical software product development is developing and finding new ways of working, the risk management methods might also require their methodologies to be updated and enhanced.

5 Discussion

5.1 List of identified future trends

The table 5 below summarizes key findings related to possible trends in implementing ISO 14971 to the medical device development. References are from reviewed research papers or regulation. If reference article is not mentioned, source was general EU regulation.

Table 5. Possible future trends

Possible future trend	**Scope**	**Scope group**	**Reference article or other (if available)**
Risk management in medical devices is rather difficult and there is a risk that the risk management process will become single, isolated process.	General risk management of medical devices.	General	Khinvasara et al. 2023, Karnika et al. 2020
Current ISO 14971 may not contain sufficient cybersecurity risk - related viewpoint and there might be some improvement needed for cybersecurity risks	Cybersecurity point of view to medical device risk management	Cybersecurity	In 2021
The use of AI has brought a whole new viewpoint to the development of medical devices and also for risk management of medical devices	The increased use of AI related to medical devices and risk management	AI	EU 2024
EU regulations are increasing, and this will most likely have an affect to the workload and also training needs for quality personnel working with medical device related issues	Medical regulatory training	Human	
The development of technologies used for medical devices (like cloud-based software development tools) requires new guidance and possibly also new definitions related to regulatory borders	Risk management related to validation of product development tools for medical devices	General	FDA 2025
Currently EU regulation related to risk management of medical	Taking human factor - issues into more	Human	

Possible future trend	Scope	Scope group	Reference article or other (if available)
products is more technical and there might be a need for defining also non-technical, human-centric issues and methodologies related to risk management	concern in risk management		
Increased integration of ISO 14971 into other relevant standards	Risk management standard	General	Yang 2024, Javanmardia et al. 2024
Managing software changes in incremental software development of SaaS-type of medical product will require more attention when software becomes more complicated	Managing incrementation changes in SaaS software development	General	Odaibo 2021, EU 2023a
The increasing complexity of SaaS-type of software product may lead to need for enhancing collection of user feedback for risk management purposes	Collecting user feedback for risk management of SaaS	Human	Ojanen 2024
The importance of identifying software components and mapping risks will remain important issue in the future.	Identifying process components and possible risks	General	Sharma et al. 2024
The software development moves towards higher levels of automatization and automatic creation of regulatory requirements	Software development of medical devices and risk management integration	AI	Häppölä 2024, Peltokorpi 2023, Lähteenmäki et al. 2023, Svempe 2024
Since there are many standards related to patient safety, there is a need for some kind of upper level control for ensuring better alignment of different standards	Alignment of different patient safety related standards may require upper level control	General	Meijer 2021, Han et al. 2020, Björnsdóttir 2024
Cybersecurity brings the need of alignment of cybersecurity risk management with medical software risk management and expanding the scope of	Cybersecurity risk mitigations	Cybersecurity	Ajax 2025, Carmichael et al. 2025

Possible future trend	Scope	Scope group	Reference article or other (if available)
risk management actions			
Instead of national and regional medical device regulatory standards, the use of general global standards and regulations would be better for medical software intended for global markets	Global perspective on medical regulation of medical software products	General	Foram et al. 2020
In addition to legacy medical software products, there is a need for similar guidance document for in-house developed medical software	Guidance related to in-house medical products	General	Lagerburg et al. 2025
Because of fast technology development and evolving medical regulation, requirements for qualified product development personnel will increase in the future	The relationship between regulatory needs and personnel competence	General	Beckers at al. 2021
In order to succeed, all company personnel must be highly involved to the applying and integration of the risk management process	Applying risk management process for developing medical software product	General	Kheir 2023, Nolan et al. 2024

According to previous table, there are some trends visible and general risk management issues are most common in referenced research papers. Since the development process of medical software devices is getting more complex, the need for automated tools was also mentioned. Risk management -thinking must be expanded from traditional product risks of physical products to cover all kinds of risks related to software products and software product operating environment. EU regulation is also constantly changing according to needs and technological development. Globalization makes also requirements for global regulation instead of regional regulation. This might be especially important with SaaS products which can be used from anywhere in the world. Identifying possible new risks caused by cybersecurity issues was also mentioned.

5.2 List of identified trends

According to this study, the implementation of quality management system (according to ISO 13485) including the risk management (according to ISO 14971) requires extensive amount of work.

Especially with SaaS-type of medical product development, the complexity of medical software may present challenges. Since the quality management standard and risk management standard give guidelines to implement the management systems, there are some extra challenges related especially SaaS-type of medical software. Increasing regulations puts pressure on company employees to learn new regulations, tools and technical issues. Because of more complex environment, risk management thinking shall be expanded also from technical issues also to human issues.

SaaS-type of medical software is typically more connected and more complex than normal, on-site and isolated medical software. Therefore, different cybersecurity issues must be addressed in a more specific and detailed way. Since the risk management standard ISO 14971 concentrates only on general risk related issues, the efficient implementation of managing cyber risks may require extra planning. Although there are separate standards and frameworks for managing cyber risks (like ISO 27001), implementing cyber risk management especially with medical software is somehow an issue with not so specific guidelines and instructions.

According to search for possible future trends, it was found out that there are many separate standards guiding the product development of a medical software product. However, the importance of connecting those separate standards may be an important issue in the future. This is because of the confidentiality of patient data and patient health issues.

Maybe the main future trends can be summarized in four main topics:

- Global perspective to medical device regulatory
- The need for alignment for various guidances and standards
- Better adoption of fast-evolving cybersecurity issues to software medical products
- Increased automation of risk management -related tasks in the development of medical software

Possible main future trends of risk management are shown at the Table 6 below. The table includes possible future trends and possible drivers and driving force which may influence the trends.

Table 6. Possible main future trends

Possible main future trend	Possible driver	Scope	Current regulation status	Driving force	Reference article or other (if available)
Instead of national and regional medical device regulatory standards, the use of general global standards and regulations would be better for medical software intended for global markets	Global markets	Global perspective on medical regulation of medical software products	EU has own medical regulation, other market areas have their own regulation	Globalization	Foram et al. 2020
Since there are many standards related to patient safety, there is a need for some kind of upper level control for ensuring better alignment of different standards	The increasing number of standards, regulation and guidance	Alignment of different patient safety related standards may require upper level control	In EU, medical directive including the number of guidance documents, national instructions and other standards is increasing	Integration of medical regulation	Meijer 2021
Cybersecurity brings the need of alignment of cybersecurity risk management with medical software risk management and expanding the scope of risk management actions	Increased complexity of medical software and cloud environment	Cybersecurity risk mitigations	Software running in cloud service is getting more complex bringing	Increased complexity caused by cybersecurity	Ajax 2025
The software development moves towards higher levels of automatization and automatic creation of regulatory requirements	Software development of medical devices and risk management integration	AI and automation	The use of AI is increasing, and more automation is used in software development, the increased regulation requires more work which could be automatized	Increased regulation and automation tools	Häppölä 2024, Peltokorpi 2023, Lähteenmäki et al. 2023, Svempe 2024

The main trends are explained in more detail in the following chapters.

5.2.1 Global perspective to medical device regulatory

Since medical software products are typically sold worldwide, there might be a need for international medical regulatory instead of regional regulatory. This can be problematic since the amount of work needed to harmonize the regulatory may require work. Typical SaaS-type of medical software device can be used globally, and possible risks are also global. Therefore, the use of globally accepted standards is important.

When there are many different regulations, there might be overlapping work which may not produce any extra value for the customer. Regional regulations, instead of common global regulation, may also cause more financial expenses and delayed development of medical software products.

5.2.2 The need for alignment for various guidances and standards

Currently there are many guidance documents, standards and similar guiding documents. Although there are lots of similarities between those, the alignment of different standards was seen important. For SaaS-type of medical software device, the better alignment of risk management and other standards could improve risk management in general.

In a perfect world, things are done only once but because of many similar regulatory needs, there is probably overlapping work. Overlapping work causes extra costs and delays.

5.2.3 Better adoption of fast-evolving cybersecurity issues to software medical product

Since cybersecurity risks and technologies are evolving fast, there might be a need for better risk management especially concerning cybersecurity risk issues. Older and slower approaches may not be sufficient for detecting and reducing cybersecurity risks. Since SaaS-type of medical software products are vulnerable to cybersecurity risks, there is an efficient need for reducing especially those risks.

In addition to cybersecurity risks, the need for a wider perspective on risk management was discussed in several research papers. In addition to technical risks, human-centered aspects and financial risks must be considered in addition to new cybersecurity risks.

5.2.4 Increased automation of risk management -related tasks in the development of medical software

Since software development moves towards higher level of automation and medical regulation increases, there is a need to also automate risk management. Automation could ease the required workload and help to implement systematic approach to risk management. For SaaS-type of medical software product, possible automation of risk management could be easy to implement when implementing other automated software development processes.

Automation does not remove human role since humans are still needed for validating the results of automation. Increased automation would speed up the risk management and product development process. Similar automation is already happening in industry as a general. The problem in combining automation and risk management is the complexity of risk related issues.

6 Conclusion

Software used for medical purposes must be developed and maintained according to medical device regulation. Medical device regulation has a long, over thirtyyears of history, and EU has an extensive set of directives and guidance documents related to medical device regulation. The aim of medical regulation is to ensure patient safety.

In addition to medical device regulation, there are several standards (like quality management standard ISO 13485 for especially medical products) which are practically mandatory for manufacturers of medical devices. Standards define requirements for quality management system, including risk management. Since there are many types of medical devices, standards are more like a general framework for work and implementing requirements always requires applying and understanding regulatory requirements.

Regulatory requirements affect the whole product development life cycle from design phase to implementation, testing, delivery and post-market activities. Since patient safety is the key issue, risk management actions must be implemented to all company processes of medical device manufacturers. Inadequate risk management process may cause patient safety to be compromised, financial losses and reputation losses for the company. If product related risks are known at a very early development phase, risk mitigation is cheaper and easier than mitigating risks when the product is already delivered to customers.

Many medical products are nowadays software products and especially software, which may be executed in a cloud environment. When the manufacturer delivers the software and takes care of updates and running of the software, the customer uses software as a service (SaaS). In a cloud environment, in addition to traditional product risks, there are also new cybersecurity risks and other risks caused by new technologies.

Because of the importance of implementing the risk management process for SaaS-type of medical software product, it will be beneficial if possible future trends about implementing and using the risk management process are known. Estimating those trends may improve the reaction to possible risks, finding better risk management implementation solutions and understanding the general trends in risk management development.

Research papers were reviewed and the main future trends were about many general level improvements related to risk management issues. Although technology and medical software products are becoming increasingly complicated, according to this study it seems that the main

development trends of risk management are mainly related to general risk management issues. EU regulation has also created additional guidance related to issues which were unclear and which needed more clarification.

Since cloud-based medical software can be used from anywhere in the world, there is a certain need for global standardization. From risk management point of view, the ISO 14971 standard could be one possible global standard for ensuring that risk of medical software is taken care of. The use of global standards, instead of many national and regional standards, could also ease the workload of medical software manufacturers.

Multiple regulations, laws, standards and guidance documents might require ensuring that there is no double work and there are no gaps between different requirements. For example, there might be many cybersecurity standards which may have many similar issues. Because of the use of multiple requirements, it should be ensured that all are covered and same actions are not done multiple times.

Especially SaaS-type of medical device is vulnerable to cybersecurity risks. Since network environment is evolving fast, there is a need for constantly observing and monitoring for possible risks. Network environment also requires many kinds of co-operation with various parties, and it must be ensured that information is available to all stakeholders.

Although AI does not seem to provide any silver bullet to risk management of SaaS-type of medical software products, more complex regulation tends to lead to increased automation. The problem in implementing automated risk management according to ISO 14971, is that human intervention might still be a crucial part of risk management. Since automation cannot yet make the final decision, the role of humans in risk management is still important.

One very interesting viewpoint is the extension of the usage of ISO 14971 from medical device industry towards processing of sensitive data with AI. ISO 14971 offers tested and robust framework for managing sensitive patient health data and same principles could be applied also in more general AI applications. There might be similarities between sensitive data used in for example medical industry and in financial industry (for example; Nordea 2026), the industry could benefit from the use of single risk management standard for all sensitive data. AI applications are also typically SaaS-based and there are certain similarities in risk management.

Figure 5 below summarizes possible future trends of implementing ISO 14971 risk management in SaaS-type of medical device. According to the figure, main trend will be implementing various general advancements and improvements to risk management. Although AI tools and cybersecurity

issues are appearing, the general core risk management thinking and implementation seems to play a key role in the future too.

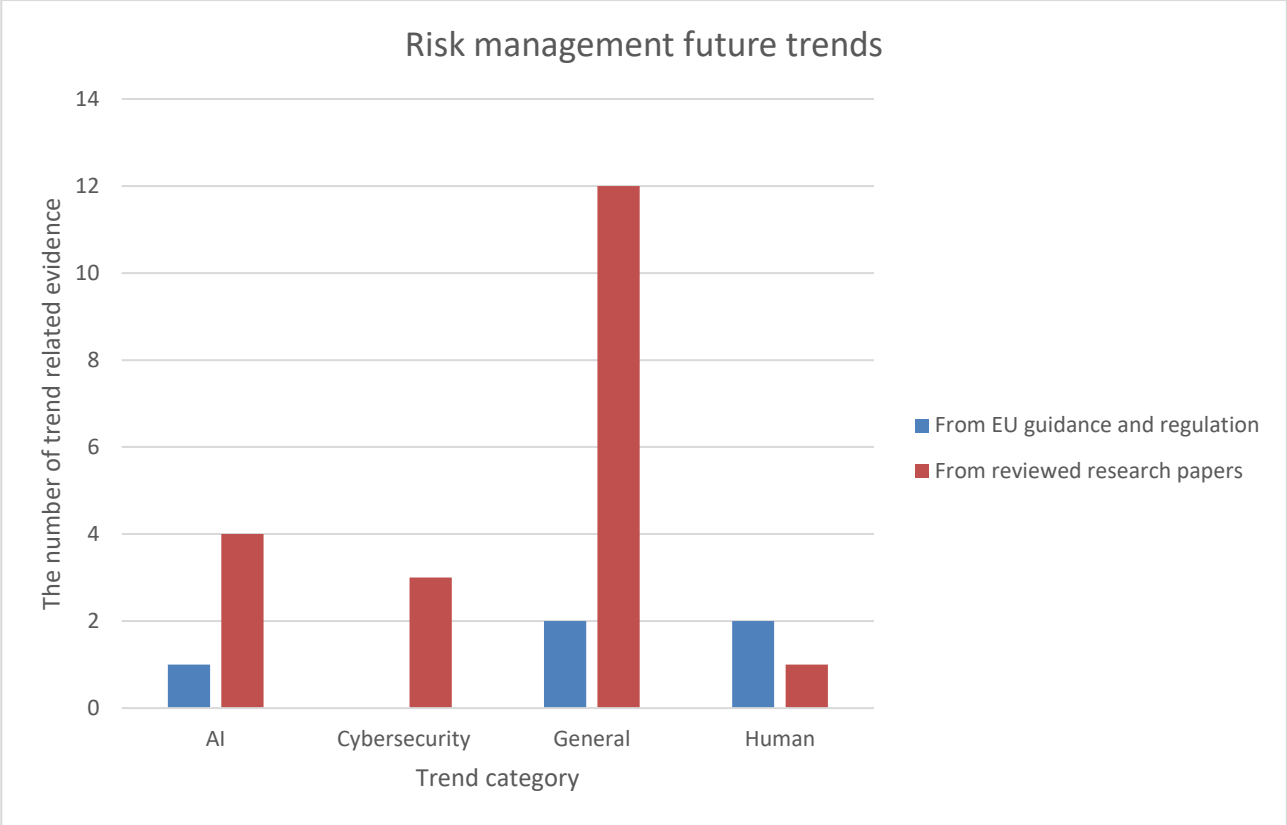

Figure 5. Summary of possible SaaS-type of medical device according to this study.

6.1 Possible subjects for further study

The limitation of this study is the number of research papers reviewed. Using more extensive literature reviews might bring broader insights. Medical device regulatory world is very complex and vast, and perhaps the research topic could be more specific. Further research could be done by automatically analyzing research papers and other relevant information.

Also, other sources like newspaper articles, professional non-academic journals and whitepapers could be added to trend estimation. If newspaper articles related to occurred risks would be added alongside with other information, the effectiveness of risk management implementation could be studied. With news -related information, it could be possible to define if risk management is

developing in the right direction. Since cybersecurity related news have become common, also medical device software related news are common.

Also reports from the medical software manufacturers could be an additional source of information and possible interviewing of relevant quality personnel could bring additional information about possible risk management future trends. However, it must be kept in mind that manufacturers might not publish any confidential information and since risk management is typically a key process in the company, companies probably do not want to give such information away. Enhancing and automating risk management actions, companies can generate more revenue and therefore interviews may not include all information. Companies also control what kind of information they want to publish, and it might be difficult to get information from, for example, problems related to risk management because company reputation issues.

There are also some databases where reported risks are stored. Those are for example:

- HPRA (Health Products Regulatory Authority) database (HPRA 2026)
- The Agence nationale de sécurité du médicament et des produits de santé (ANSM 2026)
- Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM 2026)
- The Swiss Agency for Therapeutic Products of Switzerland (Swissmedic 2026)
- The Medicines and Healthcare products Regulatory Agency (MHRA 2026)

Those databases contain information of reported risks and trends about occurred risks could be estimated from those. Since contents of risk descriptions may vary inside each database and between databases, some kind of automation would be useful for automatically retrieving and analyzing information from thos databases. Automation would have also required the implementation of some kind of complex classification algorithm.

Risk management and medical device regulation are constantly changing. It must be noted that the results of this and another related research may also have a limited lifetime. Also, one promising subject for further research could be the suitability of adopting ISO 14971 for such AI applications which will process sensitive data. This extension of the standard usage could help limiting the number of standards and expanding the use of best risk management practices also in outside medical industry.

References

AAMI Array (2023): AAMI TIR34971:2023; Application of ISO 14971 to machine learning in artificial intelligence - Guide. < https://array.aami.org/doi/book/10.2345/9781570208669 >, retrieved 10.12.2025.

AAMI Array (2024). AI/ML in Medical Devices: US & EU Regulatory Perspectives. Eric Henry. News Article 23.10.2024. < https://array.aami.org/content/news/ai-ml-medical-devices-us-eu-regulatory-perspectives >, retrieved 18.3.2026.

Ahmadi, S. (2024) Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Journal of Information Security, 15, 148-167. doi: 10.4236/jis.2024.152010. < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4775074 >, retrieved 9.12.2025.

Ajax Raymond (2025) The Future of Connected Medical Devices: Cybersecurity Risks and Quality Assurance Strategies. < https://www.researchgate.net/publication/396194310_The_Future_of_Connected_Medical_Devices_Cybersecurity_Risks_and_Quality_Assurance_Strategies >, retrieved 5.12.2025.

ANSM (2026) The Agence nationale de sécurité du médicament et des produits de santé. < https://ansm.sante.fr/ >, retrieved 18.1.2026.

Beckers R – Kwade Z – Zanca F (2021) The EU medical device regulation: Implications for artificial intelligence-based medical device software in medical physics. Physica Medica Volume 83, March 2021, Pages 1-8. < https://www.sciencedirect.com/science/article/pii/S1120179721000995 >, retrieved 16.12.2025.

BfArM (2026) Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) / Federal Institute for Drugs and Medical Devices < https://www.bfarm.de/EN/Home/_node.html >, retrieved 18.1.2026.

Björnsdóttir Svana Helen (2024) Risk analysis applied to integrate safety and security into systems design. Ph.D. Dissertation. Reykjavík University, Department of Engineering, May 2024 < https://opinvisindi.is/items/9f39c4b7-48f2-4248-bff6-3da75778e373 >, retrieved 17.12.2025.

C2A Security (2024): Shaping Risk Management in the Medical Device Industry – A Primer on ISO 14971:2019. < https://c2a-sec.com/shaping-risk-management-in-the-medical-device-industry-a-primer-on-iso-149712019/ >, retrieved 10.12.2025.

Carmichael, L. – Taylor, S. – Senior, S. M. – Surridge, M. – Erdogan, G. and Tverdal, S. (2025) Systematisation of Security Risk Knowledge Across Different Domains: A Case Study of Security Implications of Medical Devices. DOI: 10.5220/0013306100003899 In Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 1, pages 337-348. ISBN: 978-989-758-735-1; ISSN: 2184-4356 < https://www.scitepress.org/Papers/2025/133061/133061.pdf >, retrieved 3.12.2025.

EU (2017) Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.) < https://eur-lex.europa.eu/eli/reg/2017/746/oj/eng >, retrieved 11.12.2025.

EU (2019) MDCG 2019-16 - Guidance on Cybersecurity for medical devices. < https://ec.europa.eu/docsroom/documents/41863 >, retrieved 10.12.2025.

EU (2021a) Application of Regulation on Medical Devices – EU rules to ensure safety of medical devices. < https://health.ec.europa.eu/latest-updates/application-regulation-medical-devices-eu-rules-ensure-safety-medical-devices-2021-05-26_en >, retrieved 26.11.2025.

EU (2021b) Covid-19: Commission Notice on audits to be performed by notified bodies. < https://health.ec.europa.eu/latest-updates/covid-19-commission-notice-audits-be-performed-notified-bodies-2021-01-11_en >, retrieved 26.11.2025.

EU (2021c) MDCG 2021-24 - Guidance on classification of medical devices. 1 December 2021. < https://health.ec.europa.eu/latest-updates/mdcg-2021-24-guidance-classification-medical-devices-2021-10-04_en >, retrieved 11.12.2025.

EU (2023a) Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices (September 2023). < https://health.ec.europa.eu/latest-updates/manual-borderline-and-classification-community-regulatory-framework-medical-devices-september-2023-2023-09-27_en >, retrieved 26.11.2025.

EU (2023b) Add 1 - MDCG Position Paper on the application of Art.97 MDR to legacy devices for which the MDD or AIMDD certificate expires before the issuance of a MDR certificate. < https://health.ec.europa.eu/latest-updates/add-1-mdcg-position-paper-application-art97-mdr-legacy-devices-which-mdd-or-aimdd-certificate-2023-06-30_en >, retrieved 26.11.2025.

EU (2023c) Update - MDCG 2020-16 Rev.2 - Guidance on Classification Rules for in vitro Diagnostic Medical Devices under Regulation (EU) 2017/746 - February 2023. < https://health.ec.europa.eu/latest-updates/update-mdcg-2020-16-rev2-guidance-classification-rules-vitro-diagnostic-medical-devices-under-2023-02-10_en >, retrieved 26.11.2025.

EU (2023d) MDCG 2023-1 Guidance on the health institution exemption under Article 5(5) of Regulation (EU) 2017/745 and Regulation (EU) 2017/746. < https://health.ec.europa.eu/document/download/05b15d55-1bcf-4e17-99c4-15c706325847_en?filename=mdcg_2023-1_en.pdf >, retrieved 15.12.2025.

EU (2024a) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). < https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng >, retrieved 26.11.2025.

EU (2024b) Extension of the IVDR transitional periods < https://health.ec.europa.eu/document/download/dfd7a1c6-f319-4682-9bac-77bef1165818_en >, retrieved 15.12.2025

EU (2025a) Consolidated text: Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance). < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02017R0745-20250110 >, retrieved 1.12.2025.

EU (2025b) MDCG 2023-3 rev.1 - Questions and Answers on vigilance terms and concepts as outlined in the Regulation (EU) 2017/745 under Regulation (EU) 2017/746 - November 2024. < https://health.ec.europa.eu/latest-updates/mdcg-2023-3-rev1-questions-and-answers-vigilance-terms-and-concepts-outlined-regulation-eu-2017745-2024-11-11_en >, retrieved 26.11.2025.

EU (2025c) Medical Devices - EUDAMED. < https://health.ec.europa.eu/medical-devices-eudamed_en >, retrieved 15.12.2025.

EU (2025d) Medical devices –uniform application of the requirements for notified bodies. < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14471-Medical-devices-uniform-application-of-the-requirements-for-notified-bodies_en >, retrieved 15.12.2025.

EU (2025e) Proposal for a regulation to simplify rules on medical and in vitro diagnostic devices. 16 December 2025. < https://health.ec.europa.eu/publications/proposal-regulation-simplify-rules-medical-and-vitro-diagnostic-devices_en >, retrieved 17.12.2025.

FDA (2025) General Principles of Software Validation; Final Guidance for Industry and FDA Staff. < https://www.fda.gov/regulatory-information/search-fda-guidance-documents/computer-software-assurance-production-and-quality-system-software >, retrieved 26.11.2025.

Fergnani Alessandro (2019) Mapping futures studies scholarship from 1968 to present: A bibliometric review of thematic clusters, research trends, and research gaps. Futures,Volume 105, 2019, Pages 104-123, ISSN 0016-3287, < https://doi.org/10.1016/j.futures.2018.09.007 >, retrieved 19.1.2026.

Fimea (2021) Lääkinnällisiä laitteita koskeva uusi EU-asetus voimaan 26.5.2021. < https://fimea.fi/-/laakinnallisia-laitteita-koskeva-uusi-eu-asetus-voimaan-26.5.2021 >, retrieved 25.11.2025.

Fimea (2025) Fimea to investigate the conformity of software-based medical devices. 18.6.2025 | Published in English on 25.6.2025 at 13.03. < https://fimea.fi/en/-/fimea-to-investigate-the-conformity-of-software-based-medical-devices >, retrieved 18.1.2026.

Fraser AG – Redberg RF – Melvin T. (2025) The Origins of Regulations for Pharmaceutical Products and Medical Devices – What Can be Learned for the Governance of Medical Devices in Europe? European Review. Published online 2025:1-34. doi:10.1017/S1062798725000109. < https://www.cambridge.org/core/journals/european-review/article/origins-of-regulations-for-pharmaceutical-products-and-medical-devices-what-can-be-learned-for-the-governance-of-medical-devices-in-europe/04FF53F203DB0B911B1821B6749A7D7D >, retrieved 26.11.2025.

Foram Chothani – Vinit Movaliya – Khushboo Vaghela – Maitreyi Zaveri – Shrikalp Deshpande – Niranjan Kanki (2022) Regulatory Prospective on Software as a Medical Device. International Journal of Drug Regulatory Affairs Published by Diva Enterprises Pvt. Ltd., New Delhi Associated with Delhi Pharmaceutical Sciences & Research University. < https://www.researchgate.net/publication/366861809_Regulatory_Prospective_on_Software_as_a_Medical_Device >, retrieved 11.12.2025.

Gutic Bojan – Papic Tamara – Dakic Pavle (2025) Software Quality and Compliance in Intelligent Health Monitoring Systems: A Case Study of Baby FM. SQAMIA 2025: Workshop on Software Quality, Analysis, Monitoring, Improvement, and Applications, September 10–12, 2025, Maribor, Slovenia. < https://ceur-ws.org/Vol-4077/paper7.pdf >, retrieved 3.12.2025.

Han Shihui - Sinha Roopak - Lowe Andrew (2020) Assessing Support for Industry Standards in Reference Medical Software Architectures. IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society. 18-21 October 2020. DOI:

10.1109/IECON43393.2020.9255309. < https://ieeexplore.ieee.org/abstract/document/9255309 >, retrieved 17.12.2025.

HPRA (2026) Health Products Regulatory Authority. < https://www.hpra.ie/ >, retrieved 18.1.2026.

Hardian Health (2026): AI Medical Device Risk Frameworks Beyond ISO 14971. Lucy Rogers. 20.2.2026. < https://www.hardianhealth.com/insights/ai-medical-device-risk-frameworks >, retrieved 18.3.2026.

Häppölä Niko (2024) – "DevOps in Medical Device Software Development: A Multivocal Literature Review" (Discusses the limits of automation in compliance). Master's Programme in Computer Science, Helsinkin University, Faculty of Science. 24.4.2024. < https://mnfsr.gov.pk/SiteImage/Jobs/DevOps%20with%20Configuration_2024.pdf >, retrieved 3.12.2025.

I3CGlobal (2025): EU MDR Cybersecurity Requirements for Medical Device Software and MDCG Guidance. Published On - June 12.2025. < https://www.i3cglobal.com/cybersecurity-requirements-for-medical-device-software/ >, retrieved 10.12.2025.

IMDRF (2015) Software as a Medical Device (SaMD). < https://www.imdrf.org/working-groups/software-medical-device-samd >, retrieved 11.12.2025.

In Lee (2021) Cybersecurity: Risk management framework and investment cost analysis. Business Horizons Volume 64, Issue 5, September–October 2021, Pages 659-671. < https://www.sciencedirect.com/science/article/pii/S0007681321000240 >, retrieved 26.11.2025.

ISO (2006) IEC 62304:2006 Medical device software — Software life cycle processes. Published (Edition 1, 2006). < https://www.iso.org/standard/38421.html >, retrieved 5.12.2025.

ISO (2009) IEC/TR 80002-1:2009 Medical device software Part 1: Guidance on the application of ISO 14971 to medical device software. Published (Edition 1, 2009). < https://www.iso.org/standard/54146.html >, retrieved 11.12.2025.

ISO (2016) ISO 13485:2016 Medical devices — Quality management systems — Requirements for regulatory purposes. Edition 3, 2016 < https://www.iso.org/standard/59752.html >, retrieved 1.12.2025.

ISO (2019) ISO 14971:2019 Medical devices — Application of risk management to medical devices. Edition 3, 2019. < https://www.iso.org/standard/72704.html >, retrieved 1.12.2025.

ISO (2020) ISO/TR 24971:2020 Medical devices — Guidance on the application of ISO 14971. Published (Edition 2, 2020). < https://www.iso.org/standard/74437.html >, retrieved 11.12.2025.

ISO (2022) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Published (Edition 3, 2022). < https://www.iso.org/standard/27001 >, retrieved 5.12.2025.

ISO (2023) ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system. Published (Edition 1, 2023). < https://www.iso.org/standard/42001 >, retrieved 18.3.2026.

Javanmardia Ehsan – Maresovab Petra – Xiea Naiming – Mierzwiakc Rafał (2024) Exploring business models for managing uncertainty in healthcare, medical devices, and biotechnology industries. Heliyon - A Cell Press journal. Volume 10, Issue 4e25962February 29, 2024. < https://www.cell.com/heliyon/fulltext/S2405-8440(24)01993-5 >, retrieved 26.11.2025.

Karnika Singh – Praveen Selvam (2020) Medical device risk management. Trends in Development of Medical Devices, Academic Press, 2020, Pages 65-76,ISBN 9780128209608, https://doi.org/10.1016/B978-0-12-820960-8.00005-8. < https://www.sciencedirect.com/science/chapter/edited-volume/pii/B9780128209608000058 >, retrieved 26.11.2025.

Ketryx (2024): ISO 14971: A Comprehensive Guide to Risk Management in Medical Devices. Lee Chickering. November 7, 2024. < https://www.ketryx.com/blog/iso-14971-a-comprehensive-guide-to-risk-management-in-medical-devices >, retrieved 10.12.2025.

Kheir Omar (2023) Risk management and design control in the front end of medical device development. University of Antwerp, Faculty of Design Sciences Department of Product Development. Faculty of Social Sciences. Sociology Faculty of Design Sciences. Doctoral thesis. < https://repository.uantwerpen.be/desktop/irua >, retrieved 16.12.2025.

Khinvasara Tushar – Ness Stephanie – Tzenios Nikolaos (2023): Risk Management in Medical Device Industry. Journal of Engineering Research and Reports Volume 25, Issue 8, Page 130-140, 2023; Article no.JERR.105738 ISSN: 2582-2926 < https://www.researchgate.net/profile/Stephanie-Ness-3/publication/373720164_Risk_Management_in_Medical_Device_Industry/links/6553708a3fa26f66f4004d76/Risk-Management-in-Medical-Device-Industry.pdf >, retrieved 26.11.2025.

Kivimäki, Iina (2021) Development and implementation of a quality system for in vitro diagnostic medical software. Aalto University, Master's Programme in Chemical, Biochemical and Materials Engineering. Master's thesis. < https://aaltodoc.aalto.fi/items/7a1c8e3f-8c7c-4869-8530-c144db9ce61a >, retrieved 8.12.2025.

Kortelainen Tiina M – Milovanov Mikhail A. (2025) The role of ISO 9001 and ISO 13485 Quality Management System as drivers behind health technology supply chain performance and evolution. Master of Science thesis, Economics and Business Administration, University of Eastern Finland, Faculty of Social Sciences and Business Studies / UEF Business School, 03.03.2025 < https://erepo.uef.fi/server/api/core/bitstreams/165673a7-df90-4eca-8f95-4701e5687129/content >, retrieved 2.12.2025.

Lagerburg Vera – van den Boorn Michelle – Crane Reinier F – Welvaars Koen – Groen Jaap M (2025) Applying and validating a quality management system for in-house developed medical software. Front Digit Health. 2025 Apr 1;7:1461107. doi: 10.3389/fdgth.2025.1461107 < https://pmc.ncbi.nlm.nih.gov/articles/PMC11996894/ >, retrieved 15.12.2025.

LFH Regulatory (2025): How to Manage Risk in SaMD and Avoid Compliance Mistakes. May 16, 2025. < https://lfhregulatory.co.uk/how-to-manage-risk-in-samd/ >, retrieved 10.12.2025.

Lähteenmäki Jaakko, Ahola Pasi, Baraian Andrei, Förger Klaus, Granlund Tuomas, Hopia Jani, Kaikkonen Risto, Mikkonen Tommi, Niemirepo Timo, Pajula Juha, Partanen Jari, Pellinen Timo, Stirbu Vlad, Torhola Mika (2023) Agile and Holistic Medical Software Development: Final report of AHMED Project. VTT Technical Research Centre of Finland. Published - 13 Feb 2023. < https://cris.vtt.fi/en/publications/agile-and-holistic-medical-software-development-final-report-of-a/ >, retrieved 17.12.2025.

Mahamudur, Rahaman Shamim. (2022). Electrical and mechanical troubleshooting in medical and diagnostics device manufacturing: A systematic review of industry safety and performance protocols. American Journal of Scholarly Research and Innovation, 1(01), 295-318. < https://doi.org/10.63125/d68y3590 >, retrieved 2.12.2025.

MarketsAndMarkets (2025) Patien Safety and Risk Software Market Size, Growth, Shared & Trend Analysis. < https://www.marketsandmarkets.com/Market-Reports/patient-safety-risk-management-software-market-231628922.html >, retrieved 15.12.2025.

Mazov N.A. – Gureev V.N. – Glinskikh V.N. (2020) The Methodological Basis of Defining Research Trends and Fronts. Sci. Tech. Inf. Proc. 47, 221–231 (2020). < https://doi.org/10.3103/S0147688220040036 >, retrieved 19.1.2026.

Medium.com (2021): Risk Management of AI/ML Software as a Medical Device (SaMD): On ISO 14971 & Related Standards & Guidances. Blog by Dr Stephen Odaibo. < https://medium.com/retina-ai-health-inc/risk-management-of-ai-ml-software-as-a-medical-device-samd-on-iso-14971-related-standards-44ca7f3d906a >, retrieved 10.12.2025.

Meijer Wouter – Taylor Alan (2021) ISO/IEC-Standards on Quality and Safety of Telehealth Services and Mobile Medical Apps. Studies in Health Technology and Informatics, Volume290, ISSN (Print) 0926-9630, ISSN (Electronic) 1879-8365. < https://researchnow.flinders.edu.au/en/publications/isoiec-standards-on-quality-and-safety-of-telehealth-services-and/ >, retrieved 5.12.2025.

MHRA (2026) The Medicines and Healthcare products Regulatory Agency. < https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency >, retrieved 18.1.2026.

MPO Magazine (2025): AI in Clinical Software: Extending ISO 14971 with AAMI Guidance. Deepak Borole. 30.10.2025. < https://www.mpo-mag.com/ai-in-clinical-software-extending-iso-14971-with-aami-guidance/ >, retrieved 18.3.2026.

NIST (2024) The NIST Cybersecurity Framework (CSF) 2.0. < https://www.nist.gov/cyberframework >, retrieved 11.12.2025.

Nolan Niamh – McDermott Olivia (2025) Failure mode effect analysis use and limitations in medical device risk management. Journal of Open Innovation: Technology, Market, and Complexity Volume 11, Issue 1, March 2025, 100439. < https://www.sciencedirect.com/science/article/pii/S2199853124002336 >, retrieved 16.12.2025.

Nordea (2026). Nordea kirjaa uudelleenjärjestelykuluja toteuttaakseen vuoden 2030 strategiaa. 17.03-.2026 10:00. Press release. < https://www.nordea.com/fi/media/2026-03-17/nordea-kirjaa-uudelleenjarjestelykuluja-toteuttaakseen-vuoden-2030-strategiaa >, retrieved 18.3.2026.

Odaibo, Stephen G (2021) Risk Management of AI/ML Software as a Medical Device (SaMD): On ISO 14971 and Related Standards and Guidances. Cornell University, arxiv. < https://arxiv.org/abs/2109.07905 >, retrieved 28.11.2025.

Ojanen, Markus (2024) ISO 13485:2016 vaatimustenmukaisuus lääkinnällisten ohjelmistojen IT-palvelutuotannossa. Lappeenranta–Lahti University of Technology LUT, School of Engineering Science, Industrial Engineering and Management. Master's Thesis. < https://lutpub.lut.fi/handle/10024/167168 >, retrieved 28.11.2025.

Peltokorpi Mika (2023) Resilient Risk Management : case study on medical device risk management. Turku University of Applied Sciences, Master's Thesis, Health Care Technology < https://www.theseus.fi/handle/10024/806274 >, retrieved 17.12.2025.

Risk Management Association of India (2025) January 20, 2025. < https://rmaindia.org/patient-safety-and-risk-management-software-market-revenues-to-soar-by-2030/ >, retrieved 15.12.2025.

Salminen Ari (2023). Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksien tyyppeihin ja hallintotieteellisiin sovelluksiin. Teoksessa Osuva-sarja (s. 3–11). Vaasa: University of Vaasa. < https://osuva.uwasa.fi/items/f18c5d1c-c78f-4fad-8058-3c0585e66bc8 >, retrieved 18.1.2026.

Sharma Akash – Prakash Chandra – Vora Ankur (2024) Enhancing Safety and Compliance in Syringe Manufacturing: A Study of Risk Management Strategies Based on ISO 14971. Journal of Advances in Medical and Pharmaceutical Sciences Volume 26, Issue 7, Page 57-78, 2024; Article no.JAMPS.119790 ISSN: 2394-1111 < https://www.researchgate.net/profile/Akash-Sharma-5/publication/382858072_Enhancing_Safety_and_Compliance_in_Syringe_Manufacturing_A_Study_of_Risk_Management_Strategies_Based_on_ISO_14971/links/66b2096151aa0775f26c02b0/Enhancing-Safety-and-Compliance-in-Syringe-Manufacturing-A-Study-of-Risk-Management-Strategies-Based-on-ISO-14971.pdf >, retrieved 1.12.2025.

Sitra (2026). Megatrends 2026 - Towards a new social contract. Authors: Mikko Dufva, Elina Kiiski-Kataja and Jenna Lähdemäki-Pekkine. Sitra Studies 253. ISBN 978-952-347-436-9, ISSN 1796-7112. January 2026. < https://www.sitra.fi/wp-content/uploads/2026/01/Sitra_Megatrends_2026_EN_WEB.pdf >, retrieved 18.3.2026.

Svempe L. (2024) Exploring Impediments Imposed by the Medical Device Regulation EU 2017/745 on Software as a Medical Device. JMIR Med Inform. 2024 Sep 5;12:e58080. doi: 10.2196/58080. PMID: 39235850; PMCID: PMC11413540. < https://pmc.ncbi.nlm.nih.gov/articles/PMC11413540/ >, retrieved 3.12.2025.

Swissmedic (2026) The Swiss Agency for Therapeutic Products. < https://www.swissmedic.ch/swissmedic/en/home.html >, retrieved 18.1.2026.

TENK (2023) Hyvä tieteellinen käytäntö (HTK). 9.10.2023. < https://tenk.fi/fi/tiedevilppi/hyva-tieteellinen-kaytanto-htk >, retrieved 18.1.2026.

Yang, Kiki (2024) "Risk Management in Medical Devices: An application of ISO 14971," 2024 IEEE International Symposium on Product Compliance Engineering (ISPCE), Chicago, IL, USA, 2024, pp. 1-3, doi: 10.1109/ISPCE61193.2024.10541258. < https://ieeexplore.ieee.org/abstract/document/10541258 >, retrieved 28.11.2025.

Yle (2020) Potilastietojärjestelmä petti ja satoja lähetteitä jäi jumiin Kanta-Hämeessä – potilasturvallisuuden vaarantumista selvitetään. 30.1.2020 14:01 Päivitetty 30.1.2020 14:23. < https://yle.fi/a/3-11184302 >, retrieved 18.1.2026.

Yle (2023) Useiden suomalaisten laboratorioiden tietojärjestelmä ei vastaa lakia – Valvira määräsi tamperelaisyritykselle 500 000 euron uhkasakon. 6.3.2023 17:14. < https://yle.fi/a/74-20021140 >, retrieved 18.1.2026.

Yle (2025a) Potilastietoja löytyi kirpputorilla olleesta muistitikusta – asiantuntija kehottaa ihmisiä suhtautumaan asiaan maltilla. 14.1. 18:39. < https://yle.fi/a/74-20204200 >, retrieved 18.1.2026.

Yle (2025b) Fimea varoittaa huijausmainoksista: valheellinen verensokerimittari kiertää verkossa. 14.3.2025 21:10. < https://yle.fi/a/74-20149651 >, retrieved 18.1.2026.

Yle (2025c) Nobelisti Bengt Holmström sanoo suoraan: EU säätelee itsensä hengiltä – ”Tilanne on katastrofaalinen”. 27.11.2025 06:00. < https://yle.fi/a/74-20196313 >, retrieved 28.11.2025.