FeatureCloud

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

Privacy preserving federated machine learning and blockchaining for reduced cyber risks in a world of distributed healthcare

Deliverable D3.6
Manuscript on Risk management process

Work Package WP3
Guidelines, standardization, and certification

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078. Any dissemination of results reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Copyright message

Document information

Grant Agreement Number: 826078			**Acronym: FeatureCloud**	
Full title	Privacy preserving federated machine learning and blockchaining for reduced cyber risks in a world of distributed healthcare			
Topic	Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures			
Funding scheme	RIA - Research and Innovation action			
Start Date	1 January 2019	**Duration**	60 months	
Project URL	https://featurecloud.eu/			
EU Project Officer	Christos MARAMIS, Health and Digital Executive Agency (HaDEA) - Established by the European Commission, Unit HaDEA.A.3 – Health Research			
Project Coordinator	Jan BAUMBACH, UNIVERSITY OF HAMBURG (UHAM)			
Deliverable	D3.6 Manuscript on Risk management process			
Work Package	WP3 Guidelines, standardization, and certification			
Date of Delivery	**Contractual**	30/06/2022 (M42)	**Actual**	30/06/2022 (M42)
Nature	Report	**Dissemination Level**	Public	
Lead Beneficiary	2 UMR			
Responsible Author(s)	Prof. Dr Dominik Heider, UMR Roman Martin, UMR Dr. Anne-Christin, UMR Robin Gottschalk, UMR			
Keywords	Risk Management Guideline, knowledge transfer from research to industry			

Table of Content

1 Objectives of the deliverable based on the Description of Action (DoA) 5

2 Executive Summary 5
- 2.1 Methodology 5
- 2.2 Main results 5
- 2.3 Progress beyond the state-of-the-art 6

3 Risk Management Guideline 6
- 3.1 Risk Management 6
  - 3.1.1 Terminology 6
  - 3.1.2 Regulatory Requirements 7
  - 3.1.3 Normative Requirements 7
- 3.2 Academia-tailored Risk Management 9
- 3.3 Risk Management Preparation 12
  - 3.3.1 Risk Management Planning 12
  - 3.3.2 Intended Use 12
  - 3.3.3 Preliminary System Architecture 13
  - 3.3.4 Risk Policy 13
  - 3.3.5 Usability-related risks 14
  - 3.3.6 Risk Management Plan 14
- 3.4 Risk Analysis 16
- 3.6 Risk Control 20
- 3.7 Risk Monitoring 20
- 3.7 Cybersecurity 21

4 Conclusion 23

5 References 25

6 Table of acronyms and definitions 26

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

1 Objectives of the deliverable based on the Description of Action (DoA)

The objective of WP3 is to develop guidelines for a standardized software development process within the academic context and compile a documentation guideline for MDx-ready software (**Objective 1**), making the conversion from academic projects into MDx software feasible. The goal of these guidelines and recommendations is to ensure that the error rate in the diagnostic process is as low as possible. Following the quality management (D3.2) and the software life cycles process (D3.4), here in particular, as described in **Task 3**, we developed a streamlined risk management process according to ISO 14971 standard. The explicit quality report D3.5 will demonstrate a concrete implementation of such a process for the FeatureCloud project. Moreover, these guidelines will further promote the realization of regulatory requirements and training and enable control of these requirements to ensure product safety. Finally, the guidelines will be made publicly available to provide the same standards for software developed on top of FeatureCloud by third parties.

2 Executive Summary

2.1 Methodology

The procedures to detect, analyze and reduce the risk for medical devices are narrowed down in the standard ISO 14971 (application of risk management to medical devices), which describes the application of risk management to medical devices. It does not differentiate between embedded and standalone software. In contrast, the newer IEC 82304 (Health software) complements and extends it for general health software, focusing on embedded software such as apps. The IEC 82304 norm references mainly the software life cycle for medical devices standard IEC 62304 (Software life cycle processes) but allows deviation from ISO 14971. Since implementing all these norms to provide certifiable risk management is almost impossible in research institutes, we streamlined the requirements from all three norms concerning risk management to develop reasonable requirements. Additionally, key points from the ISO/TR 80002-1 that provide guidance for the application of ISO 14971:2007 and IEC 62304 were incorporated. Therefore, our proposals are derived from these standards and provide a starting point for a smooth technology transfer from an academia-tailored implementation to the medical norm. The resulting guideline delivers a feasible approach to conducting development close to the standards.

2.2 Main results

We proposed the establishment of a feasible risk management process for research organizations derived from current standards for MDx. The resulting guideline provides a risk management process that streamlines the most important and realizable activities. The guidelines focus on risk management preparation, analysis, evaluation, risk control, and risk management reporting. We are convinced that following the risk management guideline and implementing the mentioned activities improves the identification, analysis, and countermeasures against threats and potential hazards. As a result, implementing the guideline has a substantial potential to facilitate technology transfer from research institutes to industrial organizations. However, depending on specific needs, the set of activities of the risk management that work best for an organization and project may differ from our proposed guideline and should be extended or adapted. Nevertheless, the risk management guideline summarizes deliberately chosen techniques to improve a potential knowledge transfer.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

2.3 Progress beyond the state-of-the-art

While all requirements for fulfilling a medical device certification, including software as a medical device, are defined through the Medical Device Regulation and implementing standards such as the ISO 14971, they are not feasible for research units due to high requirements. In light of research organizations such as universities, scientists are often confronted with one-person-one-projects and short fixed-term contracts hindering complicated certification compliances. The main focus remains on developing prototypes (Riemenschneider et al. 2018). In particular, enforcing the establishment of machine learning and AI-based software carries out specific risk management requirements, such as considering cybersecurity issues. Here we address this issue by proposing a condensed risk management guideline that, together with our software life cycle and quality management guideline, provides a significantly lowered barrier to enable close standardized development.

3 Risk Management Guideline

The risk management pursuit aims to prevent harm to patients and users arising from conclusions, use, or treatment. Therefore, it has the utmost importance for medical devices and applications to follow the risk management (RM) requirements. The MDR determines the requirements for medical devices mainly in Annex I. It references the quality management ISO 13485 and the risk management ISO 14971. In order to develop an academia-tailored process, the various regulatory and normative activities are examined for their academic applicability. As a result, the risk management guideline contains requirements derived from multiple standards.

3.1 Risk Management

3.1.1 Terminology

By definition, Medical devices impact patients' health, including the potential negative consequences. Colloquially, these negative impacts are referred to as risks. Although there are multiple scientific terminology definitions for risk (MacMinn 1987; Burt 2001; Raine et al. 2011), the term system of ISO 14971 is suitable for medical devices because this standard is authoritative for the RM for medical devices.

According to ISO 14971, a risk is defined as the combination of **the probability of occurrence of harm and the severity of that harm**. Harms are defined as injuries or any damage to human beings. For medical devices, this refers primarily to patients. But also, the user of the medical device can be hurt. Harms's definition also includes damage to property or the environment. Potential sources of harm are called hazards. A potential risk will be estimated by the probability of the occurrence of hazardous situations multiplied by the severity of harm resulting from this situation. The harm's severity refers to the damage's intensity (ISO 2020). Different severity degrees can be used to classify harms. The severity is typically determined from insignificant to catastrophic at different levels [11, p. 90]. For example, a small scratch in the car's paint would probably be negligible damage. A fatal injury to a patient, on the other hand, would be catastrophic damage. Any situations in which a hazard can occur are called hazardous situations. The entire causal chain must be considered to identify the probability of damage. Usually, an initial event is at the beginning of this chain.

To guarantee the safety of medical devices, manufacturers must establish procedures and activities to deal with all possible risks. The totality of these procedures and activities implemented for a particular organization is termed **risk management**. These activities usually involve analyzing, evaluating, and controlling hazards and hazardous situations (Becker et al. 2019). A risk management process describes the exact sequence of steps to be performed. The procedures must be recorded in various documents in accordance with the quality management system (Hauschild et al. 2021). The execution of the procedures must also be documented, and the resulting artifacts are

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

also called records. The totality of all implemented RM processes in an organization, including the interaction with the processes of other regulatory activities, is called the risk management system.

3.1.2 Regulatory Requirements

The MDR has extensive requirements for risk management and the safety of medical devices. The general safety and performance requirements are defined mainly in Annex I. From these requirements, one can implicitly and explicitly derive risk management activities. Medical devices should be safe and effective, and medical devices should be sought. If this is not possible, appropriate protective measures should be implemented, and if necessary, these protective measures may include alarms. Alarms could warn the user or patient about possible hazards with audio-visual signals. Safety-related information can be attached if these measures also do not result in sufficient risk control. Generally, user training should also be considered. In addition, the MDR stipulates that during the post-marketing period of the medical device, it must be closely monitored whether the risk conditions of the medical device change. The MDR risk management requirements can roughly be summarized into five sub-items:

1. Planning of RM activities for each medical device.
2. Identification and analysis of hazards.
3. Estimation and evaluation of risks.
4. Elimination and control of risks.
5. Post-market monitoring.

3.1.3 Normative Requirements

MDR provides no information on the exact implementation of the prescribed requirements in practice. Standards, which are ideally harmonized, can help with this problem. The ISO 14971 standard is not yet harmonized with the MDR (European Council 2021). However, it can be a good tool for implementing an RM system because it focuses on medical devices (Catelani et al. 2011). In addition, the MDR requires utilizing state-of-the-art technology when conducting RM. Since ISO 14971 was developed by subject matter experts, is published by the ISO, and is used herein in its most current form, it can be assumed that compliance with ISO 14971 is state-of-the-art for implementing RM. According to the ISO 14971 standard, there are five general requirements for RM (ISO 2019):

- Definition of management responsibilities.
- RM competences of employees.
- Planning of RM activities.
- Establishment of an RM process.
- Filing of documentation in an RM file.

The manager of a medical device manufacturing organization shall establish a policy to determine the risk acceptance criteria along with the organizational philosophy and applicable laws and standards (Flood et al. 2015). Ideally, the policy should be coherent with the risk management policy derived from organizational quality management that defines quality goals (Hauschild et al. 2021). All required resources, such as technical and personal, as well as the assignments of responsibilities and necessary training, have to be provided. Each medical device has to be planned and documented separately. Within the planning, the scope and sequence of RM activities have to narrow down and the product life cycle they are applied. In particular, the planning must define the acceptance criteria to avoid ad-hoc decisions regarding accepting risks. The ISO 14971 suggests a procedure with six steps to remedy risks (ISO 2019):

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

1. Risk Analysis.
2. Risk Evaluation.
3. Risk Control.
4. Evaluation of Overall Residual Risk.
5. Risk Management Review.
6. Production and Post-production Activities.

During the risk analysis, the manufacturer must determine the intended use, the precise medical purpose, and the putative foreseeable misuses of the medical device. Characteristics of the product that affect safety should be identified early. Hazards and hazardous situations must be documented based on the intended use and reasonably foreseeable misuses and safety-related characteristics. In risk evaluation, the severity of damage and the likelihood of occurrence can be estimated quantitatively or qualitatively based on existing literature, similar medical devices, expert opinions, or clinical data. A decision is then made based on the estimates of whether a risk is acceptable. Risk analysis and evaluation are collectively referred to as risk assessment, followed by risk control.

For effective risk control, an inherently safe design is to be aimed. Only then should protective measures be taken. Safety information should be made available if that does not work either. After the risk control measures, the remaining risk, the so-called residual risk, should be checked for acceptance. In the case of unacceptable risks, a risk-benefit analysis can be performed to determine whether the clinical benefit outweighs the risk. All risk control measures should also be examined for completeness and potential new sources of risk. After that, it is to be examined whether the overall residual risk is acceptable. So far, the stakes have only been considered and evaluated individually.

The manufacturer shall decide whether a combination of all individual risks is acceptable. If the overall residual risk is acceptable, users should still be informed about the most crucial risks. Even a risk that the manufacturer accepts can be critical for particular users. In case of an unacceptable overall residual risk, the manufacturer should implement additional measures according to the control measures presented above. When the product is about to be released, a review should take place. It should be ensured that the RM plan has been executed correctly, that the overall residual risk is acceptable and that measures have been taken to collect safety-relevant data. This safety-relevant data shall then be collected during production and post-production. This data collection should enable the manufacturer to react to safety-critical events early. The RM process according to ISO 14971 and the usability engineering process according to IEC 62366-1 are very closely interwoven since ISO 14971 also refers to hazards caused by usability. IEC 62366-1 deals with handling and avoiding these hazards. In addition, IEC 62366-1 explicitly references ISO 14971. Usability risks must ultimately be identified, evaluated, and controlled for both standards. However, the usability engineering process is the main analysis and control of risks. After successful completion, this should then lead to the residual risk evaluation.

In contrast to ISO 14971, the normative standard for health software safety, IEC 82304, only requires a lightweight RM process. It is even explicitly mentioned that formal compliance with ISO 14971 is not required. However, the implementation of the core steps of the ISO 14971 process is recommended:

1. Intended use and operational environment identification.
2. Hazard analysis.
3. Risk estimation.
4. Risk control for unacceptable risks.
5. Post-market communication on safety and security vulnerabilities.

An ecosystem such as Google or Apple provides their application stores, interfaces, and operating systems that are not part of a standard-compliant certification process. Therefore IEC 82304 certifies

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

only the entire product. As platforms that provide basic functionalities, they cannot be reduced to a single application.

The regulatory and normative requirements are summarized and compared in Table 3.1, including a new category for a feasible academia-tailored risk management.

Table 3.1: Table of the MDR requirements, the corresponding ISO 14971 and IEC 82304 norms, and introduced groups for academia-tailored RM.

ID	RM Activity	MDR	ISO 14971	IEC 82304	Academia
A1	Intended Use	Anx. II, 1.1, 4	5.2, 5.3	4.1.a, 4.2	**1** (3.3)
A2	RM Planning	Anx. I, 3.a	4.4	-	
A3	Prel. System Architecture	-	-	-	
A4	Hazard Identification	Anx. I, 3.b	5.4	4.1.b	**2** (3.4)
A5	Risk Estimation	Anx. I, 3.c	5.5	4.1.b	**3** (3.5)
A6	Risk Evaluation	Anx. I, 3.c	6	4.1.c	
A7	Risk Control	Anx. I, 3.d, 3.f, 4	7	4.1.c	**4** (3.6)
A8	Overall Residual Risk	Anx. I, 3.e	8	-	**5** (3.7)
A9	RM Review		9	-	
A10	Production Monitoring	Anx. I, 3.e	10	-	
A11	Post-Prod. Monitoring	Art. 83; Anx. I, 3.e	10	8.4	-

3.2 Academia-tailored Risk Management

In order to develop an academia-tailored process, the various regulatory and normative activities are examined for their academic applicability. For this purpose, the requirements already identified were analyzed. Individual activities were identified and reviewed for applicability (see Table 3.1). Ten required activities and one additional activity can be derived from the regulatory and normative requirements. These activities have a sequential order. The determination of the Intended Use (A1) and the planning of the RM (A2) should always be performed at the start of the project and the RM activities. Without intended use, it is impossible to determine whether a SaMD has been developed. In addition, all risk assessments are based on the device's intended use. The RM Process must be initiated at the earliest possible stage in the development process (Flood et al. 2015). The early RM starting is relevant because hazards and error chains can only be identified through careful risk analysis. The fulfillment of acceptance criteria measures the relevance of the hazards and related risks during the evaluation phase. Only by an adequate analysis of possible risk measures can a risk-based software development approach can be pursued. In this way, new and necessary software requirements can be derived directly from the RM. Even better would be if the RM could

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

influence the design of the system directly. Therefore, the RM always initiates after the requirement analysis without a detailed system architecture. However, in academia, it isn't easy to anticipate a complete SaMD, so RM must follow a preliminary system architecture (A3). Since the academic development process is agile, recurring, and partly parallel, RM can still be well integrated (see Figure 3.1).

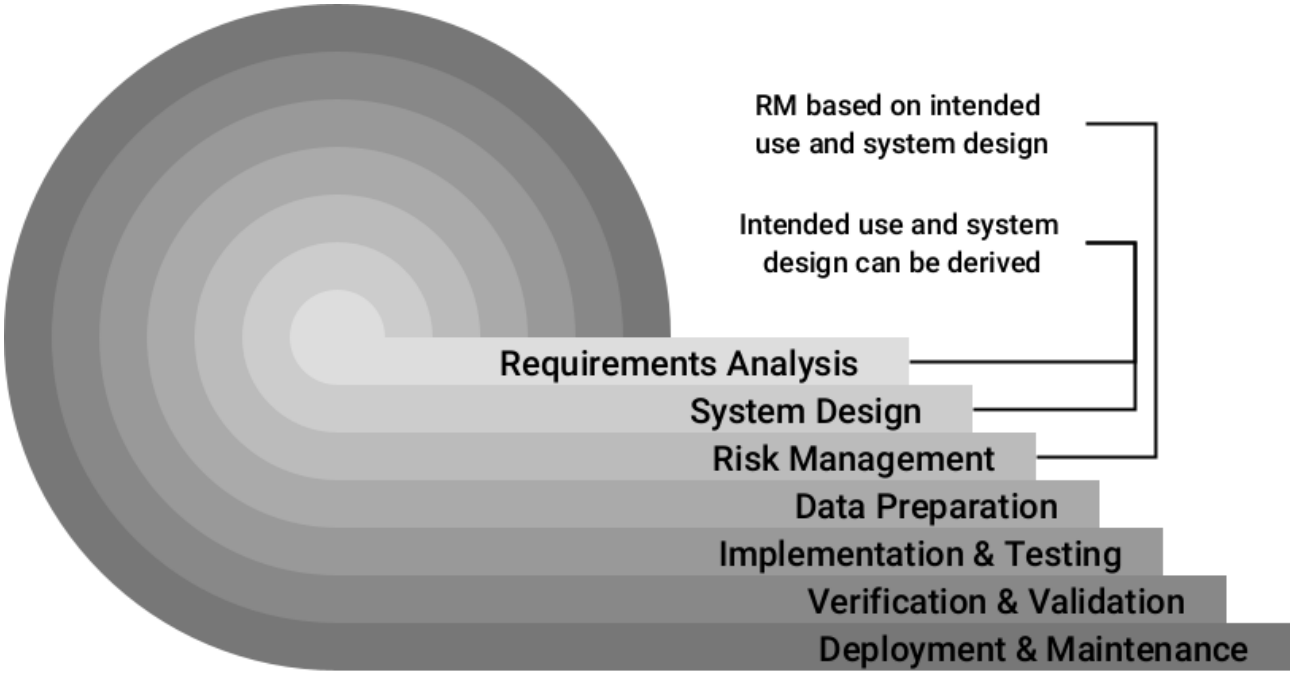

Figure 3.1: Risk management process in an agile environment.

A1, A2, and A3 constitute the RM preparation phase. Hazard identification (A4) is also possible early, but it should be done more coarsely and preliminarily. A4 is represented in the RM analysis phase in the academia-tailored process. Risk estimation (A5) and evaluation (A6) can also be carried out, but the project intentions are still to be considered vague. Simplified risk estimation and acceptance checks A5 and A6 can be represented in the risk evaluation phase of the academic tailored process. Risk control measures (A7) should only be documented and pre-planned. A7 defines the risk control phase in the academia-tailored process. Overall residual risk (A8) can only be anticipated. Evaluation and the RM review (A9) should also be done preliminarily. The monitoring during production (A10), i.e., software development, should also take place during a research project in any case. Post-production (A11) is unsuitable for the academic process due to the lack of marketability of the prototype. The process steps are explained in more detail below. Therefore, A8, A9, and A10 should build the last phase - the monitoring phase. A detailed visualization of this process can be found in Figure 3.2.

1. Preparation phase
2. Analysis phase
3. Evaluation phase
4. Control phase
5. Monitoring phase

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

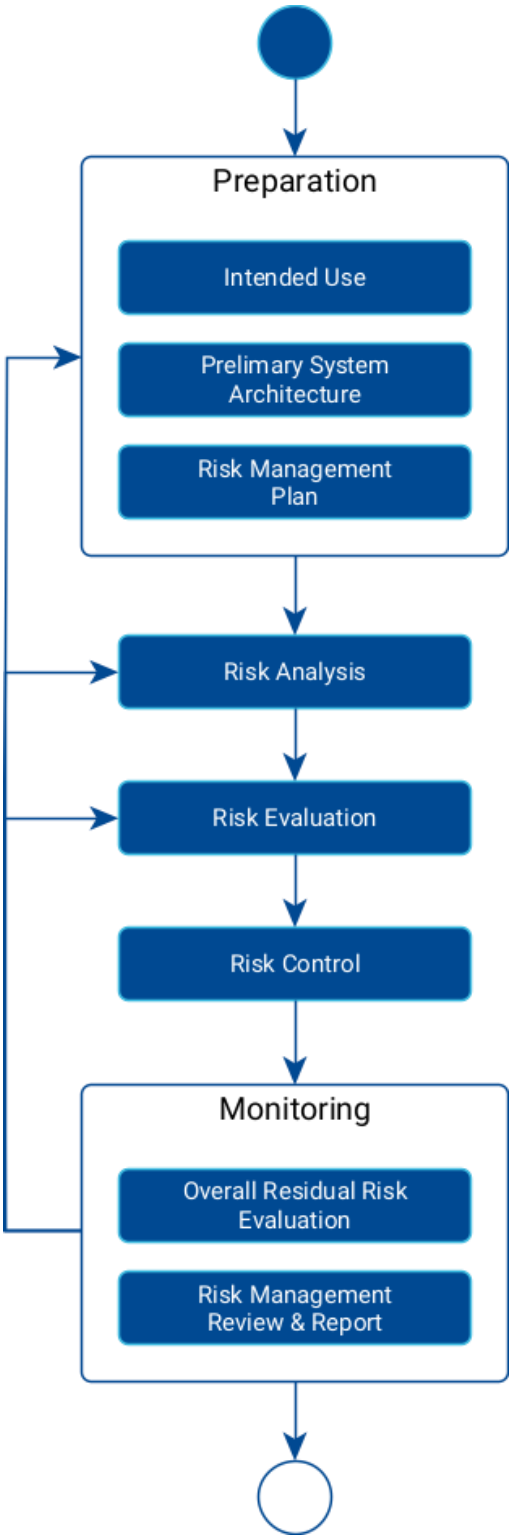

Figure 3.2: Academia-tailored risk management process, categorized into six RM activities.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

3.3 Risk Management Preparation

In the preparation phase, everything should be prepared that is required for the documentation and the RM activities. In particular, the general risk management requirements according to the ISO 14971 should be fulfilled:

- Plan all following RM activities.
- Define the intended use of a potential medical device.
- Draw a preliminary system architecture.
- Define the risk policy.

3.3.1 Risk Management Planning

The time frame of the RM activities should be precisely divided and planned. The activities should not hinder the developer in their daily work. Therefore, it is suggested to go through the RM process early in the project once in a short period to initiate all relevant documentation activities. The process is designed to run through analysis, evaluation, and control repeatedly. However, the first run-through should be pre-planned and scheduled. If there are several people involved, the format of a workshop is appropriate, in which several people jointly go through the steps of the process. However, the process is designed to be feasible for the developers. The scheduling should be done with a milestone plan in a simple table.

3.3.2 Intended Use

For regulatory affairs, the intended use takes a significant role since it affects the restrictions and requirements of a medical device. Nevertheless, since the aim is not to cover the regulatory requirements, it is essential to mention that the intended use should be described as detailed as possible. Primarily, this guideline applies to developing a well-documented prototype closely to regulatory standards. In particular, for FeatureCloud and federated machine learning, a simple prototype of a machine learning (ML) model or a small software application is not yet a Software as a Medical Device (SaMD). The definition requires a medical purpose and thus an active use in clinical practice (IMDRF 2014). However, academic prototypes can only be used in clinical research studies. Therefore, what a finished medical device could look like later on should be considered. The developer should anticipate here a finished SaMD based on his prototype. However, in a medical context, the following questions should be answered in formulated statements:

- What medical problem will be solved?
- What medical purposes can the prototype serve?
- How could the prototype be used medically?
- What could a possible use environment look like?
- Who are the users?
- Who are the patients?

Additionally, the most critical information should be presented in tabular form, the **intended use table**. Furthermore, the environment in which the software could be used should also be described. This could be, for example, the infrastructure of private practice with a Practice Management System (PMS). In addition, based on the application scenario and the application environment, it should be considered whether there are any safety-critical characteristics. For example, an application in a cloud environment could pose risks due to extensive data transfer. The medical context and the particular medical application areas should also be considered. The technological design is then continued with the preliminary system architecture.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

3.3.3 Preliminary System Architecture

The preliminary system architecture should be defined based on the project plan, intended technologies, and the requirements. It should contain roughly the individual components of the later software, such as a software architecture with a few layers in the simplest case. An example is visualized in Figure 3.3A for a basic machine learning prediction application. In this example, data and user interfaces handle all data transfer and user-related interactions, allowing users to upload necessary data for the prediction. A related backend logic passes the interaction and data to the applied machine learning model. If applicable, the preliminary architecture should be refined by adding the known underlying software and dependencies that should be used, in particular, the software of unknown provenance (SOUP), as illustrated in Figure 3.3B. The listing of SOUP is essential because developers usually have no sphere of influence on the development of this software, but they can still contribute to a chain of errors. Therefore, SOUps should also be noted and updated in a separate table to keep an overview, including the related component, the exact version, the distribution source, the author, and the intended task of the software.

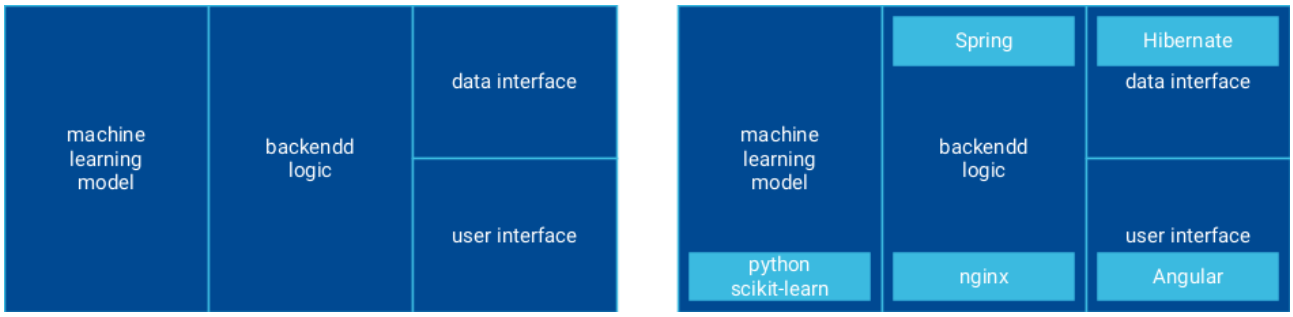

Figure 3.3A and 3.3B: Exemplarily a rough preliminary system architecture without (A) and with (B) SOUPs.

3.3.4 Risk Policy

The risk policy should be defined during the planning of the Risk Management activities at an early stage due to its high relevance for later risk decisions. Since a detailed and quantitative risk estimation is not feasible at the early stage, the simplified approach from ISO/TR 24971 should be adopted, resulting in a 3x3-fold matrix (ISO 2020). The matrix should consist of at least three levels of severity as categorized into **significant**, **moderate**, and **negligible**, and the probability of occurrence categorized into **high**, **medium**, and **low** (see Table 3.2).

A significant severity often means death or irreversible injuries, while moderate indicates a reversible injury and negligible that no or very little damage can occur. If damage could occur frequently, the probability is high. If the damage could occur a few times during the lifetime of the medical device, the probability is classified as medium. If the damage occurs very rarely, it is classified as low. The developer can now determine which risks are acceptable in a resulting risk matrix. As a rule, these are the risks in the upper right area of the matrix. The developer can also set up a more detailed risk matrix if required. In addition, the researcher should always explain, based on his intended use, why he considers the risk matrix and the acceptance criteria to be suitable. The explanation can also be in an elaborated statement.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

Table 3.2: An exemplary risk matrix with defined acceptance assessments.

	Negligible	**Moderate**	**Significant**
High	acceptable	not acceptable	not acceptable
Medium	acceptable	acceptable	not acceptable
Low	acceptable	acceptable	acceptable

3.3.5 Usability-related risks

For all usability-related risks, a separate usability engineering process can be initiated. This is mandatory for regulatory compliance of a possible SaMD application. In an academia-tailored approach, the usability specification during the start usability engineering process could be directly incorporated into the description of the intended use and the potential SaMD environment. The risk analysis could then be performed again separately for usability-related risks only. However, the usability hazards should be documented in both processes. In the end, a decision should be made in the academia-tailored usability engineering process as to whether all necessary and practicable improvements in usability have taken place. Because the usability engineering process is time-consuming, the documented usability measures arrive late. The academia-tailored RM process then addresses these measures in the monitoring phase and checks whether they fit into the overall concept of the application. This is done during the overall residual risk evaluation.

Since the scope of this guideline is the risk management process, only the interfaces regarding the risk management with the usability engineering process are visualized in Figure 3.5. The interfaces are derived from the activities of ISO 14971 (ISO 2019) and the IEC 62366-1 (ISO 2015) adapted to our academia-tailored guideline.

3.3.6 Risk Management Plan

The detailed description of the intended use, the system architecture, the risk policy, the planned schedule that includes the involved persons, and dates for the single activities should be narrowed down in the risk management plan document. Ideally, an RM file should be created that references all related documents. In contrast to that, alternatively, the RM plan can also be used as a central document containing all documentation. A better approach is to use a document management system, as mentioned in our quality management guideline (Hauschild et al. 2021).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

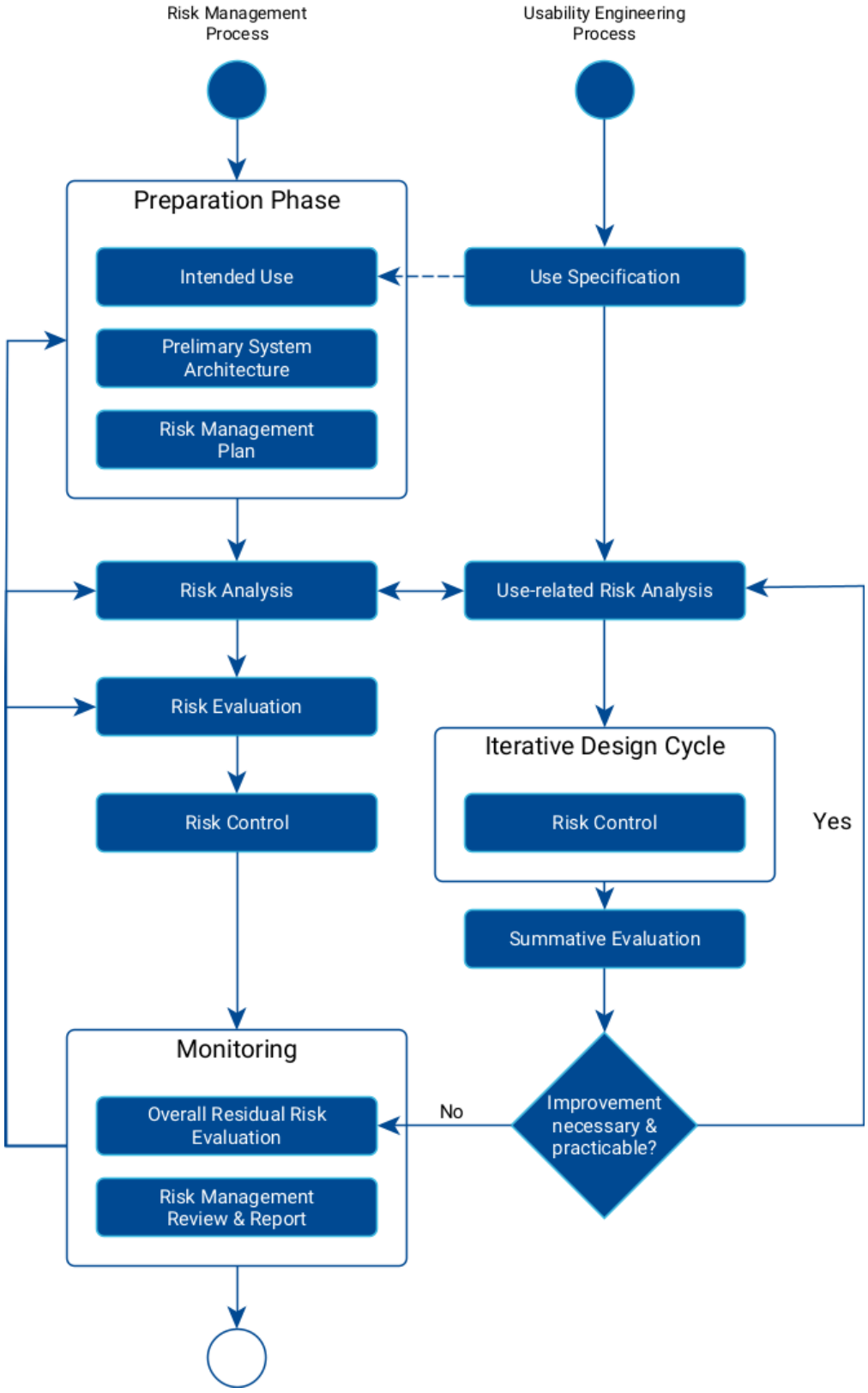

Figure 3.4: Combination of academia-tailored risk management and usability engineering processes with the relevant interfaces between both.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

3.4 Risk Analysis

The risk analysis is facing the issue of identifying putative hazards, which is especially difficult in software since the software can not have any direct physical effects and can hurt nobody. Software receives data and information processes them according to prescribed logic and results in outcoming data. However, the faulty output of the software can be part of a chain that leads to a hazard (Hastenteufel and Renaud 2019). For SaMD, initial errors in the software can lead to later hazards. Therefore, a causality chain will start directly in the software.

For software as a medical device, the creation of an error chain is even more challenging. The software output of a SaMD mainly serves people in the context of CDSS and mobile medical apps. In CDSS, information then leads to a direct impact on the physician's diagnosis and decision on treatment. In mobile medical apps, the patient is the user and then decides to self-treatment himself. The consequences are ultimately incorrect treatment or no treatment. This, in turn, results in risks to patient health. Material damage to property is inconceivable with CDSS and mobile medical apps. A particular case is damage to intangible property, that usually consists of a collection of information. Since software applications can cause illegal access, manipulation, or deletion of data, they can damage intangible property. Also, manipulation of software systems, for example, through cyberattacks, can damage or even cause total failure of an entire software system (Catelani et al. 2011; MDCG 2019). Violation of data protection, i.e., each individual's right to informational self-determination, can also be interpreted as damage to property (Moore 1998; Ballantyne 2020). The General Data Protection Regulation (GDPR) regulates the handling of personal data in the EU. Especially in the case of critical data such as health data, high hurdles apply to processing private patient data [61, p. 6]. In addition to the damage to software systems and confidential data, intellectual property infringement should also be mentioned (Lavenue 1997). Especially with extensive data collections and databases, usage rights and violations play a significant role (Chang and Zhu 2010) - this is a potential hazard derived from the input data.

For simplicity, the developer can assume here that there are five types of hazards respectively sources of harm for decision-supporting systems:

- Patient health harm due to no treatment (H1)
- Patient health harm due to incorrect treatment (H2)
- Manipulation of other systems by faulty information (H3)
- Violation of data protection and privacy (H4)
- Violation of intellectual property (H5)

The hazards H1 and H2 affect the treatment resulting from SaMD output information, while H3 means any kind of faulty output can lead to faulty states in other systems (unexpected behavior), for example, if a system does not respond or work properly anymore. But it can also be seen as part of a further chain of errors or events when output information is used as input by other systems in medical treatment. However, this is an exceedingly non-deterministic process that is difficult to predict. Since H1 and H2 already cover health-related harm, H3 affects only the system itself. H4 can arise in several ways. Furthermore, private data can leak directly from the system. Incorrect output data and faulty requests can cause other systems to manipulate, process, or delete personal data as part of system manipulation. Also, the SaMD itself could access data that may not be processed under privacy law. Similarly, H5 affects access to data protected under licensing law. For H4 and H5 in particular, the SaMD's inputs must, therefore, always be taken into account. We can now simplify this hazard chain and identify three potential sources of hazards from software:

- No output can lead to H1
- False output can lead to H1, H2, H3, H4
- Unauthorized input can occur and lead to H4 and H5

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

A visualization approach for this hazard and harm framework at SaMD is shown in Figure 3.5. Often, the causes can also be classified by the following scheme (Hastenteufel and Renaud 2019):

- Lack of usability
- Lack of interoperability
- IT security
- Software errors (incl. wrong classification)

In this context, classification or regression errors from machine learning models must be seen as software errors. A comprehensive preliminary system architecture can facilitate the identification of components in which an initial error could occur. Therefore, the developer should perform a fault-tree analysis (FTA), similar to Figure 3.6. At the root of the tree, only the aforementioned hazards are included. The hazard is back-traceable to an initial fault at the bottom. A logical gate notation can be used to visualize the error chain. This notation representation can combine causal chains with AND and OR gates together. A successfully identified initial error should be noted in the table, including the initial error, the potential hazard, and damage. This **risk table** can be expanded by adding columns for severity and probability classification as well as control measures. This procedure can be complemented by the failure mode and effect analysis (FMEA), where individual failures and their risk effects are also considered.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

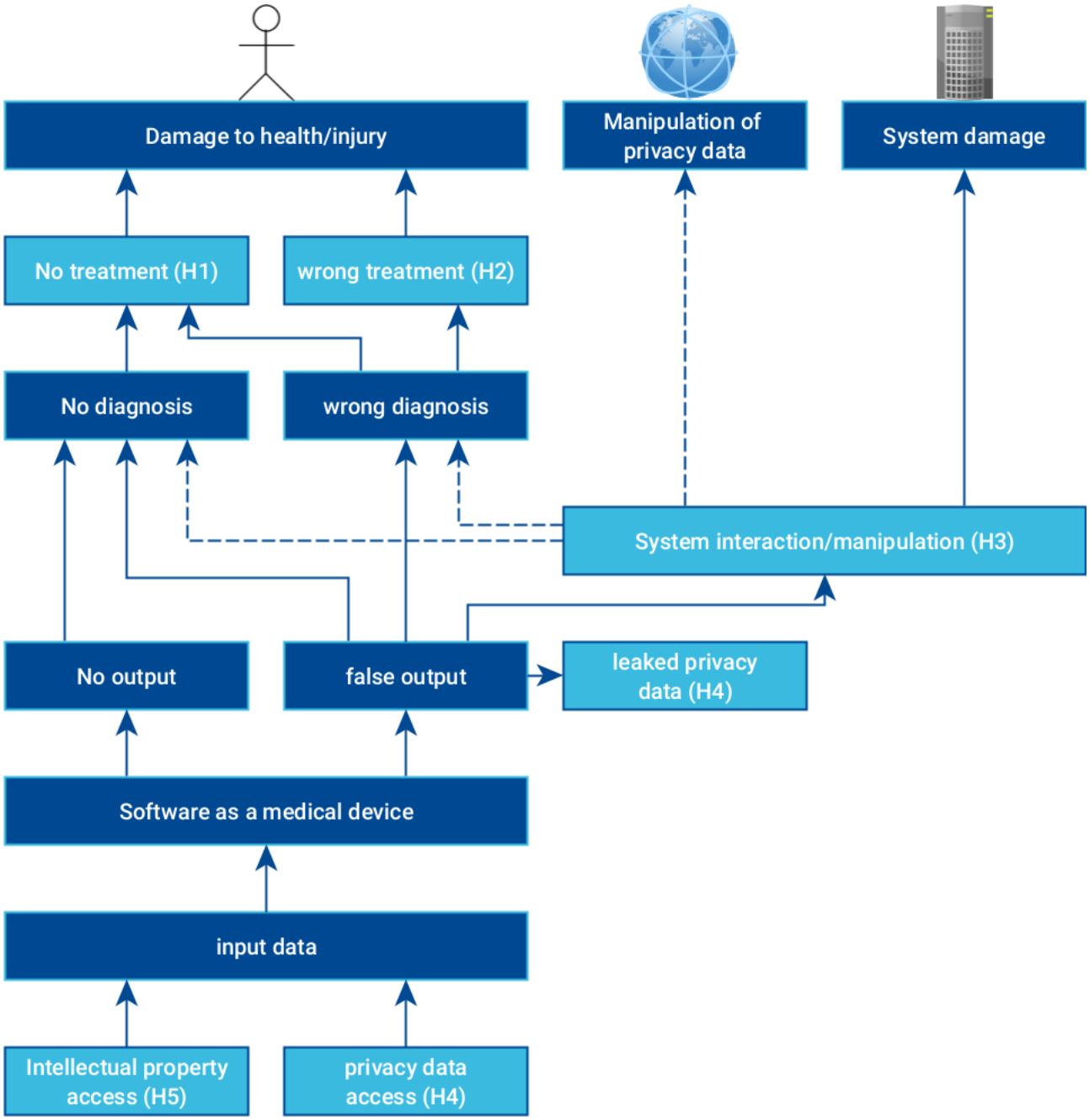

Figure 3.5: An exemplary simplified framework for harms and hazards of a Software as a medical device.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

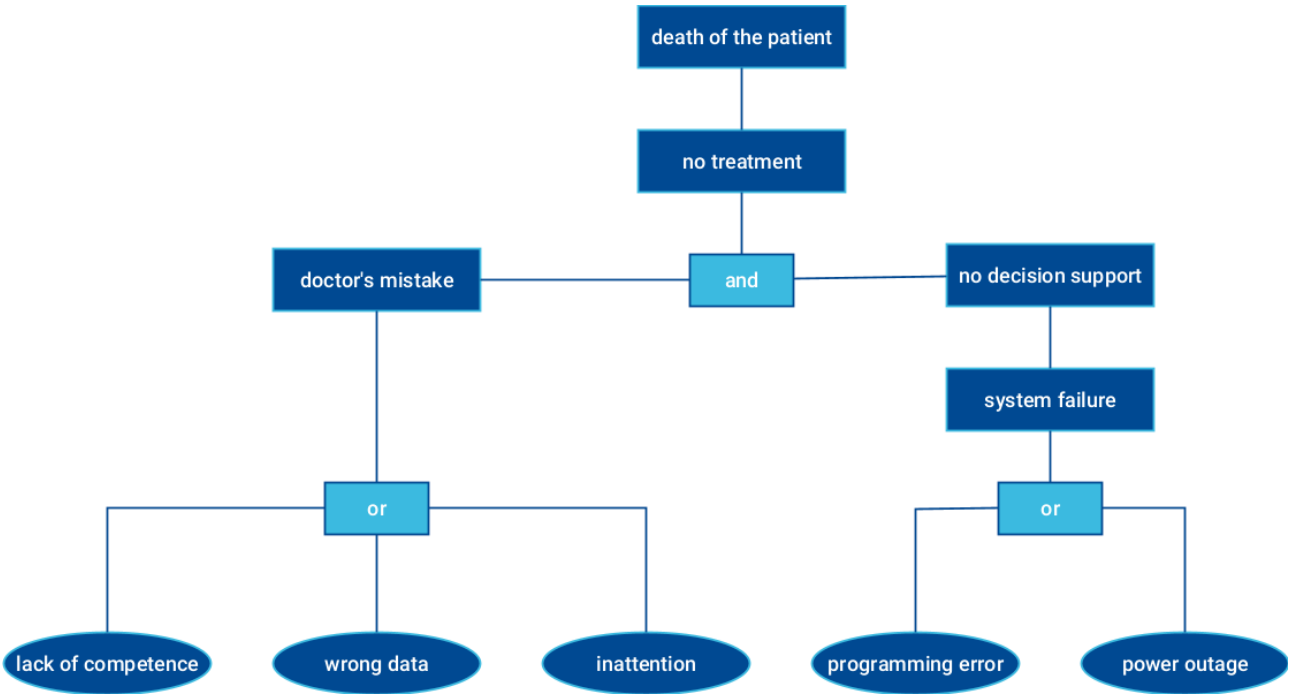

Figure 3.6: An exemplary simplified False-Tree Analysis for a clinical decision support system, showing multiple hazards and consequences.

3.5 Risk Evaluation

The risk evaluation activity aims to qualitatively estimate severity and probability according to the risk policy from the RM preparation phase. As a very deliberate estimation, the probability estimation should be derived closely from the identified risk from the risk table and how frequently it occurs. However, it is more crucial for the assessment to justify the frequencies of occurrence than to be precise. Therefore, it is legitim to make assumptions in the estimation. Estimating the damage is much easier, so it can be quickly determined whether a severe injury occurs from the intended use and use environment. For example, an app that analyzes X-ray images of broken hand bones is unlikely to result in death if it provides incorrect information. An app that analyzes X-rays of pneumonia patients is quite different. Here, wrong or no treatment can lead to significant irreversible damage or even death. In addition, both the software safety class and the MDR class of the product can be determined here.

Based on the risk matrix (Table 3.2), a new risk matrix should be created and updated, including the number of classified risks occurrences. Furthermore, the risk table should be updated, including the severity and probability estimation and if the risk is acceptable according to the risk policy.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

3.6 Risk Control

All potential risks should be reduced or eliminated by realizing risk control measures during the risk control activity. Although all risks should be addressed, the not acceptable risks should be addressed first since those measures could significantly affect other risk origins. Generally, all measures have to be explained in detail and documented. The measures considered should adhere to the prioritization scheme of the MDR and ISO 14971:

1. Control through security and safety by design
2. Protective measures if control through design not applicable
3. Providing information

Therefore, the system architecture should be aimed first, followed by software-based measures to mitigate the risks. If both approaches are not sufficient, implement instruction to the users and provide information about the potential risk. This should be mainly considered in the usability engineering process. Overall, the developer should ask themselves the following questions:

- Which measures are feasible during the project?
- Which measures are theoretically feasible but not during the project?
- Do measures lead to the obstruction of the actual project?
- Are there highly critical and not controllable risks that make it impossible to continue the project?

Every risk should be addressed and documented by at least one risk measure. All risk control methods and their implementation status should be recorded in a **risk control table** (see Table 3.9) and checked whether the measure is sufficient to reduce the risk. New requirements and their implementation should be tracked and documented as well.

3.7 Risk Monitoring

Since extensive post-production monitoring in research units is mostly not feasible, the focus is on general risk monitoring. In the beginning, all overall residual risk has to be checked to see if they are acceptable. This can be achieved by following all hazards paths in the hazards and harms framework (Figure 3.5) and evaluating if they are acceptable. The outcoming decision must be justified and written down. In case of only acceptable risks, the software development can begin and include clinical data if available. For Software as a medical device, the benefits of a potential application often outweigh the medical risks.

However, the developer should conduct a review of the risk management activities, including the previously created documentation. The documentation and a brief assessment of the RM process should be summarized in a risk management report that includes at least:

- Intended use table
- Risk table
- Risk control table
- Overall residual risk evaluation
- Summary and a short evaluation of the risk management process
- An explanation if and why the development should be continued or started.

In regular intervals, this risk management report can be updated and supplemented since this report could serve as an approach for a research transfer. Therefore, this report should summarize the RM process and activities. It serves as a guideline and reference for the whole RM process.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

Developers should be constantly alerted to changes in the development, implementation, associated research projects, and application scenario. Consequently, periodic checks should be done to consider re-entering the analysis phase. Using an RM schedule with fixed dates for the monitoring and review to avoid performing all RM activities again for each detected change is beneficial. At each scheduled review activity, the following questions should be answered at least:

- Has the Intended Use changed?
  If so, the preparation phase should be rerun since the RM was fundamentally based on the old intended use.
- Has the system architecture changed?
  If so, the researcher should incorporate this into a new risk analysis to identify sources of risk from new system components.
- Has a control measure been finally implemented?
  If so, the mitigated risk evaluation should be rerun and the Preliminary Risk Control Table completed.
- Is there new clinical data?

Clinical data can influence the risk assessment and make acceptance of critical individual risks possible. This should be taken into account in a new risk evaluation. The monitoring phase and its checks are visualized in Figure 3.7.

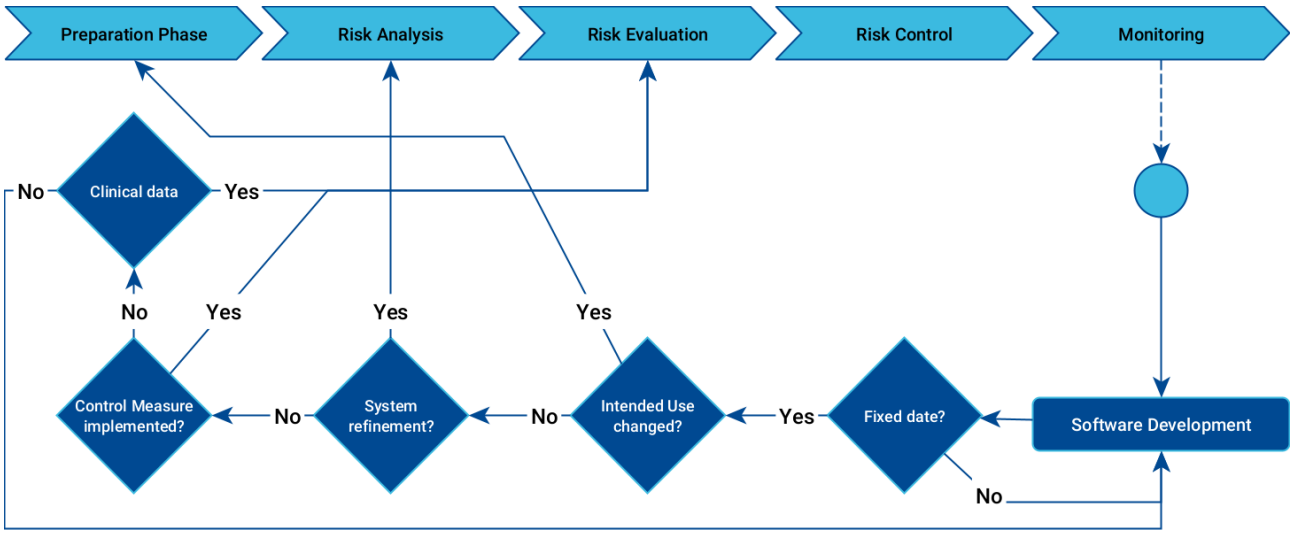

Figure 3.7: The risk monitoring phase of the academia-tailored RM process.

3.7 Cybersecurity

Although cybersecurity is not explicitly mentioned in the Medical Device Regulation, it takes on several requirements a critical role. According to a document from the Medical Device Coordination Group Document, addressing the cybersecurity for medical devices, the MDR poses requirements for the infrastructural IT-Security, Operation Security, and Information Security in the pre-market and post-market monitoring activities (MDCG 2019). The key concepts involved in the cybersecurity, specifically for the medical devices, are following the CIA principles:

- **C**onfidentiality of information at rest and in transit
- **I**ntegrity about the information authenticity and accuracy
- **A**vailability of processes, devices, data, and connected systems.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

Generally, cybersecurity can be achieved with comprehensive requirements referring to state-of-the-art threads and potential resulting hazards and harms. Current laws such as the Cybersecurity Act and the GDPR increase the requirements on cybersecurity. Both laws enforce the principles of Security by Design and Security by Default, playing a major role in the system architecture and software life cycle. Respectively to our guideline, cybersecurity should always be a key component in the preliminary system architecture, the risk analysis, risk control measures, and the risk monitoring, mainly regarding software updates. According to the suggestions from the MDCG, an explicitly incorporated cybersecurity risk management process is visualized in Figure 3.8. In particular, risk control measures related to cybersecurity should be reflected in the general risk analysis and risk control measures, which are not directly related to cybersecurity, should be considered to be analyzed deeper in a cybersecurity risk analysis. This follows the idea that any potential risk control measures could impact the cybersecurity and vice versa, cybersecurity measures affect general risk issues.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

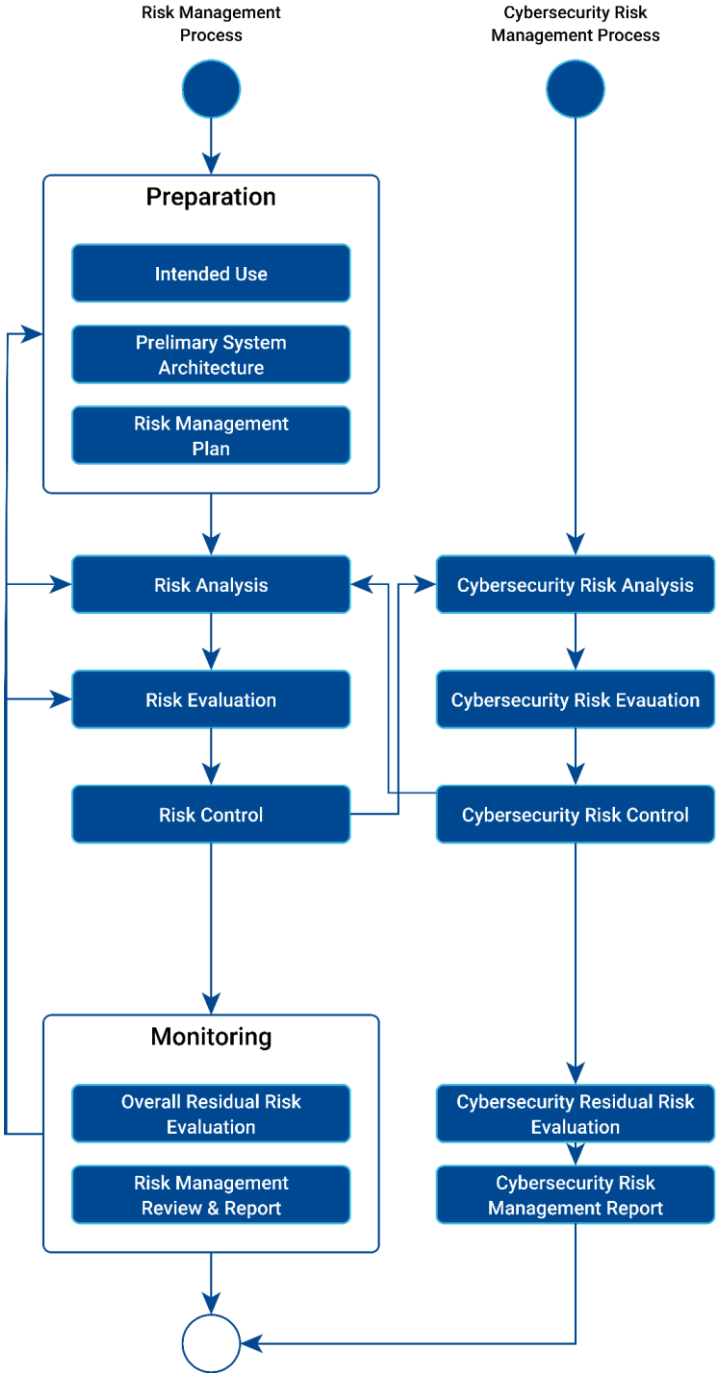

Figure 3.8: Our suggested risk management process with the proposed cybersecurity risk management process from the MDCG (MDCG 2019).

4 Conclusion

We analyzed and elaborated a likely technology transfer regarding risk management in this deliverable from research to industrial manufacturing, focusing on medical devices. For that purpose, we suggest a guideline derived from current regulations and norms that can facilitate a technology transfer by reducing the required number of steps to a feasible and predictable way for research institutes. These strict regulatory, normative, and academic requirements are here pooled into a five-step process approach. It is advisable to achieve comprehensive guideline compliance to start the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

risk management at the project beginning. In particular, it is necessary to specify an intended use and a brief preliminary system architecture at an early stage. By that, an early hazard and risk analysis are possible. Moreover, the present guideline provides a simplified framework for the hazards and harms of SaMD. Thus, health damages are caused by false or no decision information of the CDSS. However, damages could harm intangible property, such as systems, private data, and intellectual property. Using process visualization and tree graphs, how the error chains are connected and where they originate could be shown. Implementing the essential RM steps in a short period makes it possible to initiate all necessary documents early. Moreover, compact risk analysis and evaluation for a False-Tree application could be shown, and special risks of an intensive care unit could be addressed. Evaluation and control are complex at such an early starting point but can be done preliminary with the current guideline. The RM-based requirements can be identified and planned for the subsequent development process. The RM documents are constantly updated and summarized in a report in a monitoring phase. This report forms the starting point for the later research transfer, where hopefully, not all regulatory and development processes start anew.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078.

5 References

Ballantyne, Angela. 2020. “How Should We Think about Clinical Data Ownership?” *Journal of Medical Ethics* 46 (5): 289–94. https://doi.org/10.1136/medethics-2018-105340.

Becker, Kurt, Myriam Lipprandt, Rainer Röhrig, and Thomas Neumuth. 2019. “Digital Health–Software as a Medical Device in Focus of the Medical Device Regulation (MDR).” *It-Information Technology* 61 (5–6): 211–18.

Burt, Brian A. 2001. “Definitions of Risk.” *Journal of Dental Education* 65 (10): 1007–8. https://doi.org/10.1002/j.0022-0337.2001.65.10.tb03442.x.

Catelani, M., L. Ciani, S. Diciotti, F. Dori, and M. Giuntini. 2011. “ISO 14971 as a Methodological Tool in the Validation Process of a RIS-PACS System.” In *2011 IEEE International Symposium on Medical Measurements and Applications*, 408–12. https://doi.org/10.1109/MeMeA.2011.5966726.

Chang, Junli, and Xuezhong Zhu. 2010. “Bioinformatics Databases: Intellectual Property Protection Strategy.” *JIPR Vol.15(6) [November 2010]*, November. http://nopr.niscpr.res.in/handle/123456789/10687.

European Council. 2021. “Commission Implementing Decision (EU) 2021/1182.” *Official Journal of the European Union*, Official Journal of the European Union of 16 July 2021 on the harmonised standards for medi- cal devices drafted in support of Regulation (EU) 2017/745 of the European Parliament and of the Council 64, , no. L 256: 100–102.

Flood, Derek, Fergal McCaffery, Valentine Casey, Ruth McKeever, and Peter Rust. 2015. “A Roadmap to ISO 14971 Implementation.” *Journal of Software: Evolution and Process* 27 (5): 319–36. https://doi.org/10.1002/smr.1711.

Hastenteufel, Mark, and Sina Renaud. 2019. *Software als Medizinprodukt. Entwicklung und Zulassung von Software in der Medizintechnik*. Heidelberg, Germany: Springer Vieweg.

Hauschild, Anne-Christin, Lisa Eick, Joachim Wienbeck, and Dominik Heider. 2021. “Fostering Reproducibility, Reusability, and Technology Transfer in Health Informatics.” *IScience* 24 (7): 102803. https://doi.org/10.1016/j.isci.2021.102803.

IMDRF. 2014. “Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations.” https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf.

ISO. 2015. “IEC 62366-1:2015. Medical Devices - Part 1: Application of Usability Engineering to Medical Devices.” *International Organization for Standardization*.

———. 2019. “ISO 14971:2019.” *International Organization for Standardization*. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/27/72704.html.

———. 2020. “ISO/TR 24971:2020. Medical Devices - Guidance on the Application of ISO 14971.” *International Organization for Standardization*. https://www.iso.org/standard/74437.html.

Lavenue, Lionel M. 1997. “Database Rights and Technical Data Rights: The Expansion of Intellectual Property for the Protection of Databases.” *Santa Clara Law Review* 38 (1): 1–64.

MacMinn, Richard D. 1987. “Insurance and Corporate Risk Management.” *The Journal of Risk and Insurance* 54 (4): 658–77. https://doi.org/10.2307/253115.

MDCG. 2019. “MDCG 2019-16 - Guidance on Cybersecurity for Medical Devices.” *Medical Device Coordination Group Document*, 46.

Moore, Adam D. 1998. “Intangible Property: Privacy, Power, and Information Control.” *American Philosophical Quarterly* 35 (4): 365–78.

Raine, J, L Wise, S Blackburn, H-G Eichler, and A Breckenridge. 2011. “European Perspective on Risk Management and Drug Safety.” *Clinical Pharmacology & Therapeutics* 89 (5): 650–54. https://doi.org/10.1038/clpt.2011.28.

Riemenschneider, Mona, Joachim Wienbeck, André Scherag, and Dominik Heider. 2018. “Data Science for Molecular Diagnostics Applications: From Academia to Clinic to Industry.” *Systems Medicine* 1 (1): 13–17. https://doi.org/10.1089/sysm.2018.0002.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826078.

6 Table of acronyms and definitions

CDSS	Clinical decision support system
concentris	concentris research management GmbH
FL	False-Tree
GDPR	General Data Protection Regulation
GND	Gnome Design SRL
MDCG	Medical Device Coordination Group
ML	Machine learning
MS	Milestone
MUG	Medizinische Universitaet Graz
Patients	In this deliverable, we use the term “patients” for all research subjects. In FeatureCloud, we will focus on patients, as this is already the most vulnerable case scenario and this is where most primary data is available to us. Admittedly, some research subjects participate in clinical trials but not as patients but as healthy individuals, usually on a voluntary basis and are therefore not dependent on the physicians who care for them. Thus, to increase readability, we simply refer to them as “patients”.
PMS	Practice Management System
RI	Research Institute AG & Co. KG
RM	Risk Management
SaMD	Software as a medical device
SBA	SBA Research Gemeinnützige GmbH
SDU	Syddansk Universitet
SLC	Software Life Cycle
SOUP	Software of unknown provenance
UHAM	University of Hamburg
UM	Universiteit Maastricht
UMR	Philipps Universitaet Marburg
WP	Work package

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826078.