A Case Study on Data Protection for a Cloud- and AI-based Homecare Medical Device

Philipp Bende[1], Olga Vovk[2], David Caraveo[1,3], Ludwig Pechmann[3] and Martin Leucker[1,3]

[1]University of Lübeck, Lübeck, Germany, Institute for Software Engineering and Programming Languages
[2]Tallinn University of Technology, Tallinn, Estonia, School of Information Technologies, Department of Health Technologies
[3]UniTransferKlinik Lübeck GmbH, Lübeck, Germany

Abstract

To improve the treatment of many diseases, continuous monitoring of the patient at home with the ability of doctors to interact with individual cases demands an increasing number of medical devices connected to the cloud. To support the doctor's duties, such devices may benefit from AI-based diagnosis routines. In order for such devices to be approved and placed on the market, they need to comply with various legal, regulatory, economic, and social requirements. An integral part of these requirements is the protection of the patients' data.

In this paper, based on a current use case, we describe a workflow on how to identify risks and address their mitigations. To this end, we recall the relevant legal, regulatory, economic, and social data protection requirements. We pursue our findings on a Homecare OCT device that is intended to be used by elderly patients on a daily basis, by taking images of their eyes and sending them for further analysis to a cloud- and AI-based system. The patient's ophthalmologist gets notified for further dedicated treatment depending on the result. To perform the risk management, we describe (i) the architecture of the homecare system, (ii) analyze its data flow, (iii) discuss several vectors of attack, and (iv) propose ways to mitigate the risks.

Keywords

Data Protection, Risk Management, Homecare Medical Devices, Cloud- and AI-based System

1. Introduction

The rapidly developing field of medical devices using Artificial Intelligence (AI) has great potential in the healthcare domain by revolutionizing diagnosis, treatment, and patient care delivery. AI-based medical devices and software can help clinicians diagnose patients' health problems more accurately, assess risk, and provide a higher level of support for health care professionals. Such devices can also help patients by providing better, more affordable and convenient health care. Despite the benefits that can be achieved, using technologies also

This work has been conducted in the project "ICT programme" which was supported by the European Union through the European Social Fund.

43rd International Conference on Application and Theory of Petri Nets and Concurrency June 19 - 24, 2022, Bergen, Norway

bende@isp.uni-luebeck.de (P. Bende); olga.vovk@taltech.ee (O. Vovk); d.caraveo@unitransferklinik.de (D. Caraveo); lpechmann@unitransferklinik.de (L. Pechmann); leucker@isp.uni-luebeck.de (M. Leucker)

raises concerns and one of them is personal data protection. To achieve the proper level of protection comprehensive measures shall be taken. These include considering legal, technical and administrative measures.

This article gives an overview of the requirements associated with data protection applicable in the health care field and provides an example of translation of the requirements to practice. In this work we present a case study of a homecare medical system and discuss risks concerning patient data protection associated with such a system, as well as ways to mitigate these risks in practice.

We created an overview of publications that address the question of data security in medical devices and AI. Based on our findings, we can divide publications into papers that focus on legal aspects of data protection and technical aspects. The first category includes papers that focus on analyzing the legal requirements and frameworks. For example, in the article "The European Legal Framework for Medical AI" [21], the authors look into relevant laws, focusing on data protection. Nevertheless, this and similar papers use a theoretical approach. In contrast, we bring to the reader's attention requirements and related regulations but mainly focus on the practical implementation of those rules. In the second category we put articles focused on technical aspects, specifically medical devices cybersecurity. For example, the article "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0" [17] focuses mainly on cybersecurity and technical aspects, such as encryption methods. Based on this literature analysis we found out that research on the practical implementation of the requirements in real-life devices and comprehensive description of risks related to data protection is missing. Also, we would like to point out that papers are often focused on medical devices and networks located in hospitals and are usually more protected. In contrast, our work is dedicated to the home monitoring device that is used outside of a secure hospital environment and this usage can bring additional risks to data protection.

The article is structured as follows. In Section 2 we discuss legal, regulatory, social and economic requirements that need to be taken into account while dealing with personal data and requirements for data protection in software as a medical device. Following, Section 3 gives an overview of the homecare cloud system, including architecture and data flow in the system. Next, in Section 4 we describe potential risks associated with personal data protection in the current system and methods to mitigate those risks. Finally, in Section 5, we discuss the main findings.

2. Requirements

Personal data has a great value nowadays and to ensure its protection various requirements are implemented. In this article, we describe legal requirements, common and general rules that are set by law; regulatory, requirements that are set by specific normative acts in the field; economic requirements, that have a business impact; and social requirements, that include additional protection measures from sensitive personal data, such as medical and health care related data.

2.1. Legal Requirements

In order to harmonize legal requirements across European countries, the European Commission introduces the General Data Protection Regulation (GDPR) - a new law in the privacy protection field that is mandatory for all EU countries. This regulation is universal for EU countries and does not require additional implementation in the national legislation system. Although, if needed, countries can issue laws on the national level that complements GDPR[8].

Personal data is the central term in data protection laws. One of the core obligations under GDPR is to provide an adequate security level for personal data. Those measures include but are not limited to the following: ensuring confidentiality, integrity, availability of data; implementing pseudonymization, anonymization and encryption; ability to protect from incidents and minimize risks; process of testing, assessing and evaluating the system. According to Art.4 (1) GDPR "personal data" is defined as any information which is related to an identified or identifiable natural person.[8]

Data anonymization is one of the ways to keep value while preventing privacy. GDPR defines anonymisation as the "process of creating anonymous information", which means anonymized information shall not include an identified or identifiable natural person or personal data. It is important to emphasize that European legislation in the data protection field applies to personal data, which means if data is anonymized, it is out of the scope of GDPR, but it still can be a subject of other laws. Nevertheless, anonymized data or, in other words de-identified data, shall be distinguished from pseudonymized. Personal data to which pseudonymization methods were applied, that still can be attributed to a natural person shall be considered as information that may allow identification of a natural person [8]. In addition, the controller shall assess whether a person is identifiable. To do that, according to the Recital 26 GDPR, "account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly" [8].

The Article 29 Working Party (WP29) Opinion on Anonymization Techniques, based on Directive 95/46/EC, understands anonymization as "results from processing personal data in order to irreversibly prevent identification". Although, the current directive is no longer in force, the given definition is still accurate [6]. EU guidelines, such as the Working Party mentioned above, aim to provide directions toward data anonymization. However, the final decision towards using privacy methods is the responsibility of the data controller and shall be decided case by case since there is no one universal method that fits them all [23].

In addition to GDPR, some EU countries issued additional guidelines on handling data on a national level. One of the examples is Guidance on health data protection (ger. "Orientierungshilfe zum Gesundheitsdatenschutz") issued in Germany. [2] The document provides a practical overview of the essential data protection requirements for companies in the healthcare sector.

According to ENISA (European Union Agency for Cybersecurity), the choice of anonymization and pseudonymization methods depends on different parameters, primarily the data protection level and the utility of the dataset [5]. Also, the choice of a method may be concerned by the complexity associated with a certain scheme in terms of implementation, scalability and database size.

There are multiple forms to protect personal data, for example, anonymization, pseudonymization, non-disclosure, hashing, encryption or tokenization [3].

	1- Marginal	2-Minor	3-Moderate	4-Serious	5-Catastrophic
1-Frequent	acceptable	unacceptable	unacceptable	unacceptable	unacceptable
2-Occasional	acceptable	acceptable	unacceptable	unacceptable	unacceptable
3-Rare	acceptable	acceptable	acceptable	unacceptable	unacceptable
4-Unlikely	acceptable	acceptable	acceptable	acceptable	unacceptable
5-Unthinkable	acceptable	acceptable	acceptable	acceptable	acceptable

Table 1
Risk Acceptance Matrix (Probability to Severity) for the Homecare System.

2.2. Regulatory Requirements

The GDPR is a major driver for data protection which was issued by the European Commission. Prior to the GDPR, which went into effect on May 2018, manufacturers of medical devices where already challenged by data protection through the ISO 13485:2016 and the Medical Device Regulation (MDR). The MDR requires data protection in cases like clinical trials and the ISO 13485 requires that the manufacturer has to ensure the confidentiality of health information and implement the necessary methods to do so [11]. This is needed on the actual device on the one hand and also during each process, where the manufacturer would have possible access to patient data.

The ISO 13485 defines the Quality Management Systems (QMS) for Medical Devices and ensures that the product is safe, effective and efficient. Therefore, the QMS documents the whole lifecycle from the product concept, development and verification until the post market phase and to the decommissioning of a product. Each phase of the product life cycle needs to be covered by risk management activities. Manufacturers usually implement an ISO 14971 compliant risk management process to identify hazards that could result in property damage, personal injury or death of users and/or patients or even reputation loss for the manufacturer.

The ISO 14971:2012 only defines two types of risks, unacceptable and acceptable, and all have to be mitigated as far as the risk benefit ratio does not get negative. Therefore, the manufacturer has to define his risk acceptance criteria which leads to a risk acceptance matrix. The risk acceptance matrix in Table 1 shows the correlation between the probability of occurrence and the severity of a hazard. For probability there are five classes from frequent, like each use, to unthinkable, which may occur only once in the lifetime of a device. For severity there are also five classes from marginal, there is no harm at all, to catastrophic, which could lead to a severe injury or death. Therefore, a high probability and a high severity lead to unacceptable risks while on the other side low probability and a low severity may lead to an acceptable risk [12].

2.3. Economic Requirements

We can take a look at economic requirements from two perspectives. First, from the need to spend resources to apply proper measures to protect data, and second, from the possible losses in case of incompetence and data breach.

GDPR defines data controllers as a natural or legal person, public authority, agency or other body that determines the purposes and means of the processing of personal data and requires them to maintain necessary technical and organizational measures to keep personal

data protected [8]. However, considering that there is no standard set of measures that will fit all cases, and specific requirements may vary from country to country or detailed guidelines may be missing at all, in most cases it is still at the data controller's discretion to select appropriate measures. Nevertheless, applied measures shall be appropriate and relevant to the case. One of the ways to evaluate that is to conduct a risk-based data protection impact assessment. This procedure will help analyze, identify and mitigate risks associated with data processing. We want to point out that no single solution will enable data protection and data utility. It can be presented as a range of possible measures that can be implemented in specific case to find a suitable balance in each situation. This solution will depend on many factors. E.g. type and scope of processed data, risks associated with data processing, to whom data is shared and also, available resources. In each case can be defined the minimum level of protection measures applied as well as the maximum level of security that can be achieved.

The minimum level can be achieved with fewer resources, but is associated with higher risks of data loss or unauthorized access. Although, the maximum level of security provides a higher level of data protection, it also has drawbacks, such as high cost of implementation and maintenance, requirement for involvement of specialists from different fields, lower data utility associated with possible data loss resulting from anonymization or less convenient data access from a user's perspective. Violation of GDPR requirements can bring serious financial consequences for data controllers. In case of infringement of GDPR provisions, data controller can get a fine of up to 20 000 000 EUR or 4% of the total worldwide annual turnover [8]. In addition to those fines serious financial and reputation loss can be followed due to data breach. Based on IBM Security's 2020 data breach report, the average cost of a health care organization's data breach is $7.13 million, which is 10% more than in 2019 [10].

2.4. Social Requirements

According to GDPR, healthcare related data belong to the special type of data that requires additional protection measures compared to the regular personal data. This data may reveal information about the past or current status of a person's health, including physical or mental health conditions. Special information may contain results of body or tissue samples examinations, medical history, treatment details as well as data from health care professionals and medical devices [8]. Data protection requirements may also be specified in documents on a national level. For instance, Guidance on health data protection describes organizational precautions that must be taken by the companies that process sensitive health data in order to ensure the protection of this data. Those precautions include an obligation on the employees to maintain data securely, including to create a register of all data processing operations.[2]

Certainly, the secondary usage of health data, such as for research purposes, can have significant social benefits, including developing solutions that improve people's lives, providing better support in decision making, and more affordable care. GDPR specifies that personal data shall be collected for specified, explicit, and legitimate purposes and applies restrictions for the usage of personal data in a way that is incompatible with those purposes [8]. Nevertheless, processing for archiving purposes in the public interest, scientific or historical research purposes is considered compatible with the initial purposes of the collection which means data can be used for research but may require implementation of safeguard measures [8].

3. Overview of the Homecare Cloud System

Age-related macular degeneration (AMD) is an eye disease that damages the macula of the retina and leads to blurred or loss of vision in the center of the visual field. There is no cure, but treatment slows the progression of the disease and reduces vision loss.[1] Treatment is administered by injecting vascular endothelial growth factor inhibitors into the eye at fixed intervals or adaptively, if worsening of the disease is detected.[16]

The homecare system aims to develop a solution for the frequent monitoring of AMD patients' eyes and the AI-based prediction of the course of the disease. The frequent monitoring of the disease from the patient's home allows for the detection of the onset of the worsening of the disease and therefore scheduling the treatment at the best possible time. Thus, a cloud-based system that allows various different users to interact reliably and securely with multiple cloud services is realized.

When a patient is diagnosed with AMD, they can get a prescription for a homecare device. An optician provides the homecare device to the patient, who uses the device once every day to take a series of optical coherence tomography (OCT)[7] images of their eyes. These OCT images get uploaded to the cloud, where an AI evaluates the progression of the AMD and suggests whether further treatment is required. If treatment is required, the patient's doctor is notified and can make an appointment for the treatment. Additionally, the patient and their doctor can view all past images and classification results in the cloud.

3.1. Architecture of the Homecare Cloud System

Figure 1 shows an overview of the cloud system and homecare device architecture. The left part of the figure shows the typical roles of patient, doctor and homecare device in the system. These users interact with the homecare system via different interfaces. A patient can interact with the system by using the homecare device to take a series of OCT images of their eyes. The homecare device then uploads the raw images data to the cloud system. Within the cloud a preprocessing routine reconstructs a 3-dimensional DICOM-image from the uploaded data. Additionally, an AI-based classification service is notified that new images require evaluation. The classification service evaluates the image and results in a recommendation if the disease progressed and thus requires further treatment. Current and past images and results can be accessed and viewed by the patient, as well as their doctor, via a mobile application or a web front-end application.

To ensure the integrity of the patient's data in the cloud, access to the system is restricted to authenticated and authorized users. Multiple standards for authentication and authorization exist, of which the three most commonly used ones are Open Authentication (OAuth)[9], OpenID Connect[20] and Security Assertion Markup Language (SAML)[13].[15]

There is precedence of OpenID in conjunction with OAuth2.0 being used in the context high security environments such as eHealth, eGoverment and Banking[4][14].

For our implementation we utilize a server implementing OAuth2.0[9] and OpenID Connect[20]. OAuth2.0 provides role-based access control (RBAC) mechanisms therefore allowing only authorized users access to resources[9]. The OpenID Connect standard provides

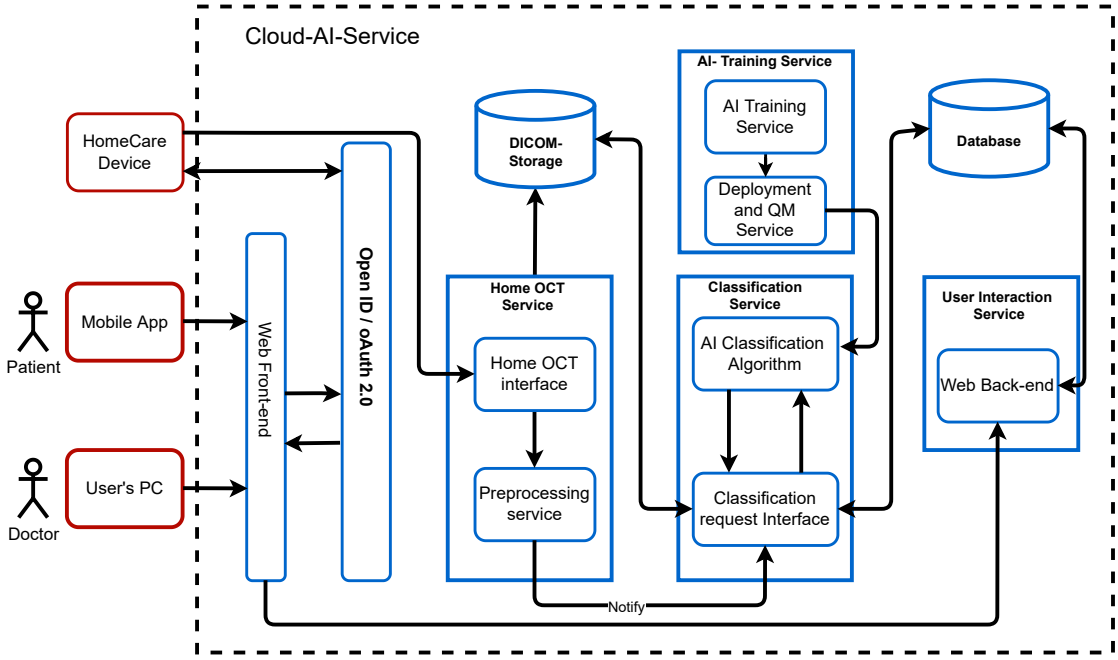

Figure 1: Overview of the cloud architecture of system and homecare device. Users (left) interact via multiple interfaces (red boxes) with cloud services (blue boxes). The services consist of interfaces for user authentication, the upload, preprocessing and AI-based evaluation of data, a service for the training and quality assurance of the AI, and interfaces for users to access the results.

web-based single-sign-on authentication and cross-domain identity management[20].

An AI-training service is used for further training and improvement, and the deployment and quality assurance of the AI-model. The AI classification algorithm runs as a cloud service and provides an interface where other services can request an evaluation of OCT images.

3.2. Data Flow in the Homecare Cloud System

To identify points of attack, where an intruder could attempt to gain access to a patient's data in the system, data- and information flow analysis can be performed. Information flow analysis results in an overview of which entities have access to the information in the system[19]. In addition to entities having access to data, a data flow analysis shows which processes and storage units have access to the data in the system[22]. Therefore, data flow analysis is preferred over information flow analysis for the identification of possible points of attack. In our data flow analysis we follow the methodology described by Seifermann et al.[22].

Figure 2 shows the data flow in the homecare system and visualizes which user is able to access the data. The homecare device (top-left) takes the patient's OCT images and sends the images, as well as metadata describing the device to a preprocessing service running in the cloud (below). The images are related to the homecare device through the metadata but not the patient.

The preprocessing service generates a 3-dimensional image file from the raw OCT image data and the device's metadata and stores it as a DICOM file in the cloud. The image files can be retrieved from the storage by specifying the storage path of the requested file. Further, the image classification service (right of the preprocessing service) gets notified about a new upload.

When notified, the classification service retrieves the image file from the storage and evaluates the contained OCT image with an AI service also located in the cloud. The classification result, whether the patient's AMD worsened or not, is combined with the patient's ID to enable a correlation between a patient and their OCT image.

The correlation between a patient, their doctor and a homecare device (above and right of the classification service) is established by the patient's optician when the patient is initially entered into the system and provided with a homecare device. The homecare device does not contain this patient identifying information.

The view result service (bottom middle) allows authenticated patients and their doctors to view an OCT image and the corresponding classification result. The user specifies the requested results (by patient.ID). The results contain the path to the corresponding image files, which are retrieved from the storage. A doctor further can view the results of all their patients (bottom right).

Figure 2 shows the data flow through the system. Data is divided into three categories by the criticality of the data. Non-Identifying Non-Biometric data does not contain sensitive information (purple). The OCT images of a patient's eye are biometric data and contain sensitive information in pseudonymized form (yellow). The patient's identifying data, like the patient's name, is shown in blue.

4. Analysis and Mitigation for Potential Risk to the Patients' Data

Following the regulatory requirements discussed in Section 2.2, risk management for the homecare medical system is implemented. This section describes the reasons for processing sensitive data, potential risks to the data, as well as the measures taken in order to minimize the risks.

4.1. Reasons to Process Sensitive Data in the System

GDPR Art. 9 protects personal and biometric data and prohibits the processing of such sensitive data. An exception is that processing can be permitted if a specific requirement for the processing, such as medical diagnosis, exists[8].

For the purpose of medical diagnosis, it is necessary to record and store the patient's full name in the system in order for their doctor to search and find a specific patient's data. When a new patient is stored in the database, it will be automatically generated an ID for this patient to guarantee the uniqueness of the database keys. Other personal information, such as age, sex or address are not processed in the system, since they are not required for the use case.

In addition to the personal identifying data, biometric data in the form of OCT-images of the patient's eyes are stored and processed in the system. It is necessary to store and process the biometric data because the purpose of the system is to detect AMD and evaluate the progress of the disease. The system creates a historical record of the patient's disease.

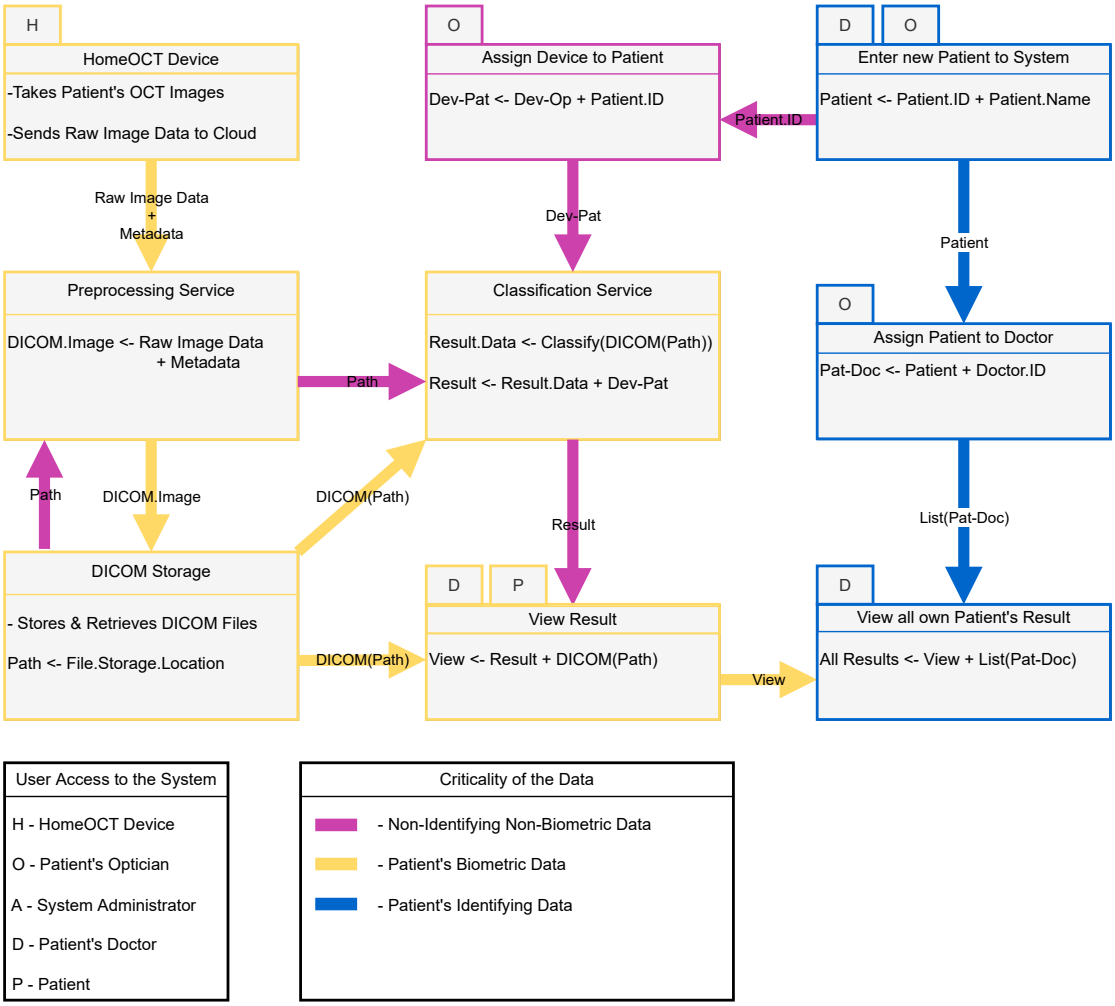

Figure 2: The data flow in the homecare system. The boxes represent functions in the cloud system. The letters on top of the boxes show which user can access the function. A user has access to all information in the accessed function including information which is derived from other functions. The arrows represent information that is passed from one function to another one.

Since an AI detects the disease, multiple OCT-images are required to train of the neural network. The original training images are not retained in the system, but only the neural net's weights are based on these training images.

4.2. Potential Risks for Patients' Data

Based on the Risk Analysis in Table 1 we identify points of attack in the data flow of the system as depicted in Figure 2, where a potential intruder or malicious user could attack the system in order to gain unauthorized access to a patient's sensitive data.

We differentiate between an intruder attempting to break into the system and a malicious

user, for example, a rogue system administrator, attempting to access sensitive patient data.

An intruder could attempt to break into the cloud system or intercept data that is uploaded from the homecare device to the cloud (see Figure 2 top left arrow). The intruder can also attempt to identify a patient and find out the patient's diagnosis.

AI-models are not protected under GDPR, however an additional vector of attack on an AI-based system is the attempt to reconstruct training data from the learned weights of the model [18]. In this scenario, an intruder could request the classification of a specific data sample and attempt to gain information about the original training images from the network's response.

A malicious user on the other hand would already have access to the system itself and could attempt to access sensitive data or the AI without authorization. Such sensitive data could be accessed by gaining access to the database storing the patient's information and diagnosis (see Figure 1 Database top right) or the patient's biometric data (see Figure 1 DICOM-Storage top middle). A similar scenario is a doctor attempting to access patients' data for which he has no authorization, such as a different doctor's patient.

Additionally, a malicious user would have access to the AI and could attempt to gain information about the training data from the network's response, similar to an external intruder but with full access to the network.

4.3. Mitigation of Potential Risks

According to Table 1 the hazards discussed in Section 4.2 are unacceptable risks due the severity of the damage and frequency of occurence and therefore need to be mitigated. Table 2 shows the mitigation strategy for each hazard in order to reduce the risks to an acceptable level.

The homecare device sends sensitive biometric data over an unsecure channel to the cloud. An intruder can intercept this communication. By encrypting all communication with HTTPS, the sensitive data cannot be recovered even if intercepted.

In order to prevent an intruder or unauthorized user from gaining access to the databases, we do not allow direct access to the database but require access through a backend service. The backend only accepts requests from users who are authenticated and authorized by the authorization server. This ensures that only authorized users can access the database and only data they have permission for.

Since a doctor must be able to access his patients' data, each patient is mapped to a doctor. The backend allows for requests from a doctor only for patients' data, for which this mapping exists. This ensures that the doctor can access his own patients' data but not to others doctors patients' data.

To ensure the security and integrity of patient's sensitive data, all patient information are encrypted in the database. Furthermore, the biometric data is pseudonymized by not mapping it to the patient's name, but an ID. This makes it harder for an intruder to de-pseudonymize a patient, since he would need to get access to both, the biometric data and the database connecting IDs to patients.

The risk to the integrity of the AI model's training data is low since the model is not publicly available and the system allows only selected users a limited number of requests. In case of the intruder having access to the model, he can only access biometric data but no information about the patient is exposed.

Hazard	Risk acceptance before mitigation	Mitigation	Risk acceptance after mitigation
An intruder tries to fetch information which is sent by the Home OCT device	Frequent × Serious ⇒ Unacceptable	• Encrypt all communication with HTTPS	Frequent × Marginal ⇒ Acceptable
An intruder attempts to break into the cloud service and accesses data	Occasional × Serious ⇒ Unacceptable	• Limit system access to authorized users utilizing OpenID and oAuth2.0 protocols • Restrict access to database only via backend service • Backend checks user validation before forwarding data	Unlikely × Serious ⇒ Acceptable
Intruder or user gets access to the database in which the patient data is stored	Occasional × Serious ⇒ Unacceptable	• Restrict access to database only via backend service • Backend checks user permission before forwarding data • Encrypt database with secure standards	Unlikely × Serious ⇒ Acceptable
A doctor can see results of other doctors' patients	Occasional × Serious ⇒ Unacceptable	• Restrict access by mapping each patient with a doctor • Allow access only to data from patients with correct mapping	Unlikely × Serious ⇒ Acceptable
A patient can see results of other patients	Rare × Serious ⇒ Unacceptable	• Restrict access by mapping each patient with a device • Allow access only to data from device with correct mapping	Unlikely × Serious ⇒ Acceptable
An intruder attempts to gain information about a patient from the database	Unlikely × Catastrophic ⇒ Unacceptable	• Encrypt all patient's sensitive data in the database • Encrypt patient's diagnosis	Unlikely × Moderate ⇒ Acceptable
An intruder tries to correlate biometric data with the patients	Rare × Serious ⇒ Unacceptable	• Pseudonymize biometric data by correlating patient's id with patient's sensitive data • Not storing patient information on the homecare device	Rare × Moderate ⇒ Acceptable
An intruder attempts to gain information about the AI's training data	Rare × Serious ⇒ Unacceptable	• Restrict allowed number of classification requests to one per day for external users • Restrict access to the weights of the AI model • Biometric training data is pseudonymized	Unlikely × Serious ⇒ Acceptable

Table 2
A sample of the risk management for the homecare system. The risk acceptance is calculated from the probability and severity of the hazard according to Table 1

5. Conclusion

Protection of personal data is a highly regulated field especially when they are used in medical devices and software. Various risks occur due to the high value of this data and its sensitive nature. Compliance becomes more challenging because of the diverse nature of those requirements and the lack of practical examples for implementation. To feel this gap, our paper demonstrates how legal, regulatory, and other requirements can be implemented on a real-life project. In detail, we describe risks and ways to mitigate them. We believe that other readers can benefit from our research by learning how theoretical requirements can be translated into practice.

In our data flow analysis, we identified two main types of attackers: intruder, a person outside the system, and malicious user, a person inside the system, e.g administrator or doctor, who tries to get access to data without authorization.

Both types can have different vectors of attack and require mitigation measures to lower potential risks. The main mitigation strategy includes the following: encrypted communication between device and cloud, limited system access, restricted access to the databases and backend check of user's permissions, access mapping between doctor and user, encryption of sensitive personal data and pseudonymization when possible, storing patient's data in database encryption with secure standards, and avoid storage on homecare devices.

Even though achieving absolute security is not physically possible, our analysis shows that the implementation of the measures mentioned above significantly mitigates the risks of a successful attack and decreases possible damage in case of intrusion.

References

[1] Apte, R. S. Age-Related Macular Degeneration. *The New England journal of medicine 385 6* (2021), 539–547.

[2] BMWI. Orientierungshilfe zum Gesundheitsdatenschutz. [Online, Accessed 15 February 2022].

[3] Datenschutz-Grundverordnung. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), April 2016. [Online; accessed 16-February-2022].

[4] Domenech, M. C., Comunello, E., and Wangham, M. S. Identity management in e-Health: A case study of web of things application using OpenID connect. In *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)* (2014), pp. 219–224.

[5] ENISA. Pseudonymisation techniques and best practices, November 2019. [Online; accessed 11-February-2022].

[6] European Commission. Article 29 working party opinion 05/2014 on anonymisation techniques.

[7] Fujimoto, J. G., Pitris, C., Boppart, S. A., and Brezinski, M. E. Optical Coherence Tomography: An Emerging Technology for Biomedical Imaging and Optical Biopsy. *Neoplasia 2(1-2)* (2000), 9–25.

[8] GDPR. Regulation (EU) 2016/ 679 of The European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such data, and Repealing Directive 95/46/EC, April 2016. [Online; accessed 01-February-2022].

[9] Hardt, D. The OAuth 2.0 Authorization Framework. RFC 6749, RFC Editor, October 2012.

[10] IBM. IBM Report: Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year. [Online, Accessed 24 March 2022].

[11] Johner, C. Datenschutz im Gesundheitswesen bei medizinischen Daten. [Online, Accessed 25 March 2022].

[12] Johner, C. ISO 14971 and Risk Management. [Online, Accessed 29 March 2022].

[13] Lewis, J. E. Web single sign-on authentication using SAML. *IJCSI International Journal of Computer Science Issues 2* (09 2009).

[14] Lodderstedt, T., Bradley, J., Labunets, A., and Fett, D. OAuth 2.0 Security Best Current Practice. Internet-Draft draft-ietf-oauth-security-topics-19, Internet Engineering Task Force, Dec. 2021.

[15] Naik, N., and Jenkins, P. Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect. In *2017 11th International Conference on Research Challenges in Information Science (RCIS)* (2017), pp. 163–174.

[16] Okada, M., Kandasamy, R., Chong, E. W. T., McGuiness, M. B., and Guymer, R. H. The Treat-and-Extend Injection Regimen Versus Alternate Dosing Strategies in Age-related Macular Degeneration: A Systematic Review and Meta-analysis. *American journal of ophthalmology 192* (2018), 184–197.

[17] Qiu, H., Qiu, M., Liu, M., and Memmi, G. Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. *IEEE journal of biomedical and health informatics 24 9* (2020), 2499–2505.

[18] Rigaki, M., and Garcia, S. A Survey of Privacy Attacks in Machine Learning, April 2021. arXiv:2007.07646.

[19] Sabaliauskaite, G., and Adepu, S. Integrating Six-Step Model with Information Flow Diagrams for Comprehensive Analysis of Cyber-Physical System Safety and Security. In *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)* (2017), pp. 41–48.

[20] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and Mortimore, C. OpenID Connect 1.0 specification, November 2014. [Online, Accessed 30 March 2022].

[21] Schneeberger, D., Stöger, K., and Holzinger, A. The European legal framework for medical AI. In *International Cross-Domain Conference for Machine Learning and Knowledge Extraction* (2020), pp. 209–226.

[22] Seifermann, S., Heinrich, R., Werle, D., and Reussner, R. Detecting violations of access control and information flow policies in data flow diagrams. *Journal of Systems and Software 184* (2022), 111138.

[23] Vovk, O., Piho, G., and Ross, P. Anonymization Methods of Structured Health Care Data: A Literature Review. In *International Conference on Model and Data Engineering* (2021), Springer, pp. 175–189.