Eco-system for disease specific clinical workflow and data integration

DELIVERABLE D1.3
Legal and Ethical Requirements

Project number:	ITEA 21026
Document version no.:	v1.0
Edited by:	Many partners
Date:	12.12.2023

ITEA Roadmap challenge:
Smart Health

HISTORY

Document version #	Date	Remarks
V0.1	02.10.2023	Starting version, template
V0.2	05.10.2023	Compilation of first input by ForteArGe
V0.2.1	19.10.2023	Inputs for MS use case from Innova
V0.3	01.12.2023	First review & feedback
V1.0	12.12.2023	Final version

TABLE OF CONTENTS

1 Introduction

In the healthcare sector, with the continuous advancement of technology, the demands on data management and protection have been increasing. The dynamic nature of modern healthcare services, the integration of clinical data, the adoption of artificial intelligence technologies, and multi-national collaborations underscore the importance of adhering to legal and ethical standards.

1.1 Aim of the Activity

This document has been crafted with the aim of ensuring that the SYMPHONY project achieves its goals while upholding individuals' fundamental rights and freedoms, ensuring data security, and operating in alignment with international standards.

In the following sections, one can find a detailed outline of the essential legal and ethical requirements for the responsible development, implementation, and management of the project. This initial draft will serve as a guideline for the SYMPHONY project and will be revised as needed in the subsequent phases of the project.

1.2 Contributors

Contribution	**Section(s)**	**Editor**
Generation of outline in draft version.	1-7	ForteArGe
Generation of v00-v01.	1-7	ForteArGe
Inputs for applicable parts for MS use case	1,2,4	Innova
Inputs for the AA use case	2-6	LUMC, Others
First revision	1-7	ForteArGe

1.3 Glossary

Affiliation	**Description**
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
CCPA	California Consumer Privacy Act
LPPD	Law on the Protection of Personal Data
AI	Artificial Intelligence
XAI	Explainable Artificial Intelligence
MS	Multiple Sclerosis
EU	European Union

2 Data Protection and Privacy

2.1 General Data Protection Regulation (GDPR) Compliance

2.1.1 Introduction

One of the most significant data protection legislations in the world has been General Data Protection Regulation. Even before it came into force in May 2018, it had been called the toughest privacy and security regulation in the world.

The reputation has been built on the fact that the regulation imposes obligations on organisations everywhere, if they handle the data of individuals in the EU and introduces severe penalties for the ones who mistreat the data. In a nutshell, the GDPR is about: penalties, the need for determining a solid legal basis for processing personal data, data protection by design and by default, data breach notification and pseudonymisation. It is composed of 10 chapters concerning: general provisions, principles, rights of the data subject, duties of data controllers and/or processors, transfers of the data to third countries or international organizations, independent supervisory authorities, cooperation and consistency, remedies, liability and penalties, provisions relating to specific processing situations, delegated acts and implementing acts and final provisions.

2.1.2 General Requirements

[R21.1] Ensure that all collection and processing of patient data complies with the international or the local relevant data protection laws of the participating countries.

- International Regulations: HIPAA (for the U.S.), GDPR (for the EU).
- Local laws: Different countries or regions might have specific rules. It's crucial to ensure you're in line with all applicable standards.

2.1.3 Use-Case Specific Requirements

UC1 PC	[R21.2] Swedish Patient Data Act (2008:355) [R21.3] Health and Medical Service Act (2017:30) [R21.4] Data cannot be stored or managed by entities that are under obligation to provide data to third party countries. For example, storage or staff belonging to American legal entities, even if the physical storage is within EU [R21.5] Any access (reading, writing or changing) to patient data must be logged with as a minimum when, who and what was accessed.
UC2 AA	[R21.6] Dutch Medical Treatment Contracts Act (in Dutch Wet op de geneeskundige behandelingsovereenkomst (WGBO; WB art. 7:446 - 7:468 BW)). This regulates the relationship between patients and care providers. [R21.7] Dutch Medical Research Involving Human Subjects Act (in Dutch Wet medisch-wetenschappelijk onderzoek met mensen (WMO). [R21.8] Dutch GDPR Implementation Act (in Dutch Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). This is the Dutch version of the GDPR [R21.9] Data can only be processed within EU and countries with adequate data protection as indicated by the EC. Countries need to be listed in the privacy documentation.

UC3 AF	[R21.10] In the Netherlands, the Data Protection Authority (Autoriteit Persoonsgegevens) is responsible for the GDPR compliance. [R21.11] Uitvoeringswet Algemene verordening gegevensbescherming" (UAVG), which translates to the "Implementation Act General Data Protection Regulation [R21.12] The requirements follow European standards. [R21.13] Data Protection Impact Assessments (DPIAs): all processing of data should be registered in advance in the registry of data processing.

2.2 Data Anonymization and Pseudonymization

2.2.1 Introduction

Whether or not data is considered to be personal data depends on the effectiveness of the pseudonymisation procedure. Consequently, retraceable pseudonymised data may constitute personal data and be subject to data protection legislation. The GDPR defines pseudonymisation as “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”

Data minimisation can be achieved with different technical solutions. One way of minimising the amount pf personal data, and thereby also adhere to the principles of the GDPR, is anonymising the data, and if not possible, by pseudonymisation. The use of the technique relates first hand to the definition of what constitutes personal data, as set out by the scope of the GDPR.

To minimize the data use, project partners should attempt to anonymise and pseudonymize the personal data as much as possible. One must consider carefully the cases where a need to retain the connection to the data subject, and why this is the case. Even for cases where the data subject can no longer be identified, ethical issues can still be present depending on the origin of the data or how it has been retained and the source of the datasets.

2.2.2 General Requirements

2.2.3 Use-Case Specific Requirements

[R22.1] (Regarding UC2 AA): Dutch GDPR Implementation Act (in Dutch Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). This is the Dutch version of the GDPR.
[R22.2] (Regarding UC4 MS & Src.): Personal patient data should be anonymized before acquisition.
[R22.3] (Regarding UC4 MS & Src.): Unique identifiers on DICOM tags such as Series UID and Instance UID should be pseudonymized while processing the data. Personal information should only be stored in the standalone mobile vision test application and shouldn't be shared with the cloud (only test results can be shared).
[R22.4] DICOM images should be deleted after AI inference process is finished.
[R22.5] Authentication should be required to access the PACS system that temporarily stores DICOM images.
[R22.6] Any access and interaction with the system should be logged.

2.3 Data Storage and Security

2.3.1 Introduction

Data security is relevant for both ethical and legal concerns. To ensure the fundamental rights and freedoms of data subjects, the obligation to protect the data and ensure proper protection of the information is key.

The higher the risk to the fundamental rights and freedoms is connected to the processing, the more safeguards need to be taken. These risks are especially connected to the type of data involved as well as the risk for unauthorized access to, or disclosure, accidental deletion or destruction of the data. The risk should be evaluated case-by-case and for high-risk activities, a clear explanation of the mitigation of the risks needs to be laid out.

2.3.2 General Requirements

[R23.1] Ensure robust encryption/anonymization/de-identification techniques are employed for data in transit.

[R23.2] Maintain regular audits to detect any potential vulnerabilities in the data storage system.

3 AI Ethics and Best Practices

3.1 Transparent AI

3.1.1 Introduction

Transparency in AI refers to the ability to peer into the workings of an AI model and understand how it reaches its decisions. There are many facets of AI transparency, including the set of tools and practices used to understand the model, the data it is trained on, the process of categorizing the types and frequency of errors and biases, and the ways of communicating these issues to developers and users.

The multiple facets of AI transparency have come to the forefront as machine learning models have evolved. A big concern is that more powerful or efficient models are harder -- if not impossible -- to understand since the inner workings are buried in a so-called black box.

Like any data-driven tool, AI algorithms depend on the quality of data used to train the AI model. Therefore, they are subject to bias or have some inherent risk associated with their use. Transparency is therefore essential to securing trust from the user, influencers or those influenced by the decision.

3.1.2 General Requirements

[R41.1] Ensure that AI models used in the project can be understood and interpreted by healthcare professionals.

[R41.2] Provide clear documentation on the data sources and training methods used for AI.

3.1.3 Use-Case Specific Requirements

UC3 AF	[R41.3] Create clear lower dimensional visualizations of the results of unsupervised clustering methods. [R41.4] Moreover, we will follow European standards in AI transparency.
UC4 MS & Src.	[R41.5] AI model will generate explainable output with heat map of the model's interest via using XAI approaches. [R41.6] DICOM viewers will display both original and lesion extracted MRI images on the same page to see the differences. [R41.7] Lesions extracted from MRI images should be clearly visible on the raw image with high contour.

3.2 AI-supported Decision Making

3.2.1 General Requirements

[R42.1] Ensure that AI models only serve as assistive tools and do not replace human judgment.

[R42.2] Maintain regular validation and updating of AI models to ensure their accuracy and relevance.

3.2.2 Use-Case Specific Requirements

UC3 AF	[R42.3] Use or create balanced data sets [R42.4] AI-supported tools will only be used for suggestions. No decisions will be based on AI.
UC4 MS & Src.	[R42.5] Visual and textual data about the dissemination of lesions in time and space can be displayed to monitor MS progression on MRI images and support decision making steps. [R42.6] Reports generated by AI algorithms should be clear and understandable to experts. [R42.7] The system should display both processed and raw images in the same view to allow experts to evaluate images from their own perspective

4 Clinical Guidelines and Best Practices

4.1 Clinical Decision Support

4.1.1 General Requirements

[R51.1] Ensure that the AI models align with accepted clinical guidelines (see Section 5.1.2 for details).

4.1.2 Use-Case Specific Requirements

UC1 PC	[R51.2] Swedish National Guidelines at Nationellt vårdprogram prostatacancer - RCC Kunskapsbanken (cancercentrum.se)
UC2 AA	[R51.3] We will follow the Dutch Clinical Practice Guideline for Abdominal Aorto-iliac Artery Aneurysms (in Dutch: Richtlijn voor Aneurysma van de Abdominale Aorta) which is based on European Society for Vascular Surgery (ESVS) Clinical Practice Guidelines on the Management of Abdominal Aorto-iliac Artery Aneurysms.
UC3 AF	[R51.4] We will follow world-wide protocols for AF treatment.
UC4 MS & Src.	[R51.5] We will follow the guidelines for MS and Sarcopenia treatment.

4.2 Medical Guideline Automation

4.2.1 General Requirements

[R52.1] Automate clinical guidelines without compromising the integrity and accuracy of clinical best practices.

[R52.2] Engage clinical experts to review and approve any automated processes derived from clinical guidelines.

5 Collaboration and Partnerships

5.1 Multi-Country Collaboration

5.1.1 General Requirements

[R61.1] Abide by the healthcare and data protection laws of all participating countries.

[R61.2] Establish clear agreements and terms of collaboration between partners from different countries.

5.1.2 Use-Case Specific Requirements

[R61.3] (Regarding UC2 AA): Contribution from non-NL participants within Philips using deidentified personal data will be organized via bilateral agreement with LUMC and approval from privacy officers. Data can only be processed within EU and countries with adequate data protection as indicated by EC - specific countries need to be listed on privacy documents.

5.2 Intellectual Property Rights

5.2.1 Introduction

As described in the SYMPHONY Project Co-operation Agreement (PCA), Article 8 - INTELLECTUAL PROPERTY AND ACCESS RIGHTS

5.2.2 General Requirements

[R62.1] Clearly define the ownership and usage rights of any technology or solution developed during the project.

[R62.2] Ensure that innovations brought about by the project are protected from unauthorized use or copying.

6 Conclusion

The SYMPHONY project is positioned to revolutionize the healthcare IT sector, and adherence to these legal and ethical guidelines will be instrumental in its successful and responsible implementation. All stakeholders should remain committed to these principles to uphold the trust and safety of the patients and professionals involved.