TREAT

Labelled in ITEA4, a EUREKA cluster, ITEA CALL 2022

ITEA3 Project Number 22022

D2.1 LEGAL&ETHICAL ANALYSIS REPORT

Due date of deliverable: Dec 2024
Actual date of submission: Jan 2025

Start date of project: 01 – 01 - 2024	**Duration:** 36 Months
Organisation name of lead contractor for this deliverable:	GLINTT HEALTHCARE S. L
Author(s):	Carlos Tercero
Status:	Final
Version number:	1.0
Submission Date:	<10-01-2025>
Doc reference:	TREAT_D2.1_LEGAL&ETHICAL_ANALYSIS_REPORT_V1.0
Work Pack. / Task:	WP2: Data Collection, Privacy and Security / Task 2.1 Legal and Ethical Analysis

Description: ***(max 5 lines)***

This task involves researching and reviewing laws and regulations related to privacy, security, and data collection in the healthcare sector, including GDPR and HIPAA, as well as country-specific regulations. It also involves identifying ethical concerns, such as handling sensitive data, informed consent, and patient autonomy. A plan will be developed to obtain consent and handle medical information securely, in compliance with regulations. This activity will be conducted continuously throughout the project to integrate legal and ethical updates into the research and development efforts.

Nature:	<Use one of these codes: **R**=Report, **P**=Prototype, **D**=Demonstrator, **O**=Other>		
Dissemination Level:	**PU**	Public	
	PP	Restricted to other programme participants	
	RE	Restricted to a group specified by the consortium	
	CO	Confidential, only for members of the consortium	**X**

DOCUMENT HISTORY

Release	Date	Reason of change	Status	Distribution
V0.1	28/12/2024	First draft	Draft	…
…	…	…	…	…
V1.0	10/01/2025	Approved by PMT, to be submitted to ITEA4	Final	…

Table of Contents

Glossary

<Please provide a description of all acronyms/abbreviations used in the document.>

Abbreviation / acronym	Description
GDPR	General Data Protection Regulation – European Union law on data protection and privacy.
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales – Spanish law complementing GDPR.
DPIA	Data Protection Impact Assessment – A process to identify and mitigate privacy risks.
ISO	International Organization for Standardization – Developer of global standards.
HIPAA	Health Insurance Portability and Accountability Act – US regulation for healthcare data protection.
PIPEDA	Personal Information Protection and Electronic Documents Act – Canadian privacy law.
FHIR	Fast Healthcare Interoperability Resources – A standard for electronic health data exchange.
XAI	Explainable Artificial Intelligence – AI systems designed to provide clear explanations for their decisions.
AES	Advanced Encryption Standard – A specification for data encryption.
CT	Clinical Team – A group of healthcare professionals involved in the project.
DT	Development Team – Engineers and developers working on technical implementation.
CIOMS	Council for International Organizations of Medical Sciences – Guidelines for ethical research.
NIST	National Institute of Standards and Technology – US agency providing standards for cybersecurity.
EMA	European Medicines Agency – Regulatory body for medicines in the EU.
WHO	World Health Organization – International public health agency.

1. Executive Summary

The TREAT (Transforming Healthcare Through Semantic Interoperability and Self-Efficacy) project aims to improve the management of Non-Communicable Diseases (NCDs) through the use of advanced technologies such as artificial intelligence (AI), semantic interoperability and interactive interfaces. NCDs represent a global challenge, responsible for 71% of annual deaths, and traditional healthcare systems are not equipped to facilitate effective self-care of these conditions. TREAT seeks to empower patients, improving their ability to manage their health through digital platforms that integrate data from wearable devices, medical records and health apps.

One of the main innovations of the project is the creation of a patient-centric platform that facilitates semantic interoperability between different types of data and health services. This enables seamless access to medical information by professionals and patients, improving clinical decision-making and fostering patient self-efficacy. The platform combines AI to generate personalized recommendations based on health data analysis, with a user interface system that uses technologies such as extended reality (XR) and advanced conversational chatbots, designed to improve patient adherence to medical treatments.

TREAT is distinguished from other solutions on the market by its ability to integrate multiple digital services into a single platform, providing a complete solution for NCD management. While current competitors, such as HumanITcare, Siemens and Philips, offer fragmented solutions, TREAT offers full interoperability between devices and systems, significantly improving the quality and quantity of care available to patients.

The project consortium is composed of partners from seven countries, covering the entire value chain of the healthcare ecosystem. However, the project has faced challenges such as uncertainty in funding in some countries, technical difficulties in system integration, and the need to comply with regulatory standards such as the GDPR. To mitigate these risks, the consortium has implemented action plans such as redistributing responsibilities among funded partners and creating dedicated technical teams for integration.

In conclusion, TREAT has the potential to transform NCD management, improving clinical effectiveness and patient self-efficacy, with the ambition to create a lasting impact on the quality of healthcare globally.

2. Introduction

Work Package 2 (WP2) of the TREAT project focuses on data collection, privacy, and security.

This WP is crucial because it provides the foundation on which the other TREAT technologies are built.

WP2's main goal is to provide components and tools for the data lifecycle, ensuring that collected data is managed securely, ethically, and efficiently.

WP2 builds on the requirements and workflows defined in WP1 to guide the data collection process.

Data collected in WP2 will feed the AI algorithms developed in WP3 and will be used to validate the technologies developed in WP4.

2.1 Objectives & Tasks

The focus areas of WP2 include:

- **Legal and Ethical Analysis (led by GLINTT):** Research and review relevant laws and regulations related to data collection, privacy, and security in the healthcare sector in participating countries. This includes analysis of GDPR and other relevant regulations.

- **Software Module Design and Implementation (led by DEXTROMEDICA S.L.):** Design and implement software modules for systematic data retrieval, collection, anonymization, and normalization. This includes the development of application programming interfaces (APIs) to access different data sources, such as wearables, electronic medical records (EMRs), and digital diaries.

- **Privacy and Security Components Design and Implementation (led by DEXTROMEDICA S.L.):** Design and implement components to ensure the privacy and security of the collected data. This includes the use of privacy-preserving techniques, such as data aggregation, anonymization, and encryption. It also involves collaborating with the Secur-e-Health (ITEA3) project to share knowledge on building privacy and security components for health data sharing.

- **Data Management Plan (led by Maastricht University):** Develop a data management plan to ensure that collected data is organised and stored securely and accessibly. This includes identifying the tools and software to be used for data management, as well as procedures for data quality control and archiving.

2.2 Deliverable Objectives

The document's main objective is to investigate and review the relevant laws and regulations related to data collection, privacy and security in the healthcare sector. This task, led by GLINTT, focuses on analysing the legal and ethical framework of the countries participating in the project.

Although the specific document is not found in the sources provided, it can be inferred that its objectives align with the description of task 2.1: "Legal and Ethical Analysis" within WP2: Data Collection, Privacy and Security.

The likely objectives of the document include:

- **Identifying relevant laws and regulations:** The report should start by identifying the specific laws and regulations governing the collection, storage, processing and sharing of health data in each of the participating countries of the TREAT project.

- **Analyse the scope and application of regulations:** The report should analyse how these laws and regulations apply to the proposed data collection and processing activities within the TREAT project. This includes assessing compliance with requirements such as informed consent, data anonymization, and patient rights.

- **Identify potential legal/ethical challenges and risks:** The report should identify any potential challenges or risks that may arise from the collection and use of health data in the context of the TREAT project.

- **Propose mitigation measures:** Based on the legal and ethical analysis, the report should propose specific measures to mitigate the identified risks and challenges. This could include developing privacy and security protocols, obtaining informed consent from patients, and establishing ethical oversight mechanisms.

3. Ethical Framework

3.1 Ethical Issues in Medical Data Collection

In the TREAT project, medical data collection involves ethical challenges due to the sensitivity of the data and the importance of protecting patient rights. Key ethical issues include:

1. **Privacy Protection:** Ensuring the confidentiality of patient data through robust security measures such as encryption, pseudonymization, and secure data transfer protocols. Data must be safeguarded from unauthorized access or breaches during its collection, processing, and storage.
2. **Transparency:** Patients must be fully informed about how their data will be used, who will have access to it, and the measures in place to protect it. Lack of transparency can undermine trust and lead to ethical violations.
3. **Purpose Limitation:** Data should only be collected for the specific purposes defined in the project scope, such as improving healthcare recommendations or generating AI models. Collecting excessive or irrelevant data can raise ethical concerns.
4. **Equity and Bias:** Ensuring that data collection methods are inclusive and do not disproportionately exclude certain populations or introduce biases into the datasets, which could impact the fairness of AI-driven healthcare recommendations.

3.2 Informed Consent

The TREAT project places significant emphasis on obtaining informed consent to ensure ethical compliance and patient trust. The key elements of the informed consent process include:

1. **Clarity and Accessibility:** Consent forms and information must be written in clear, non-technical language that is easy for participants to understand. Multilingual options and assistance should be provided when necessary.
2. **Voluntary Participation:** Participants must have the freedom to choose whether to participate without any form of coercion or undue influence. They should also have the right to withdraw consent at any stage without facing consequences.
3. **Detailed Information:** Patients must be informed about:
    - The purpose of the project.
    - The specific data being collected.
    - How their data will be used and protected.
    - Any potential risks and benefits of participation.
4. **Digital Consent Mechanisms:** TREAT incorporates secure digital tools to facilitate the consent process, ensuring that patients can provide, review, or revoke their consent conveniently and securely.

3.3 Patient Autonomy

Patient autonomy is a cornerstone of the ethical framework within the TREAT project, ensuring that patients retain control over their healthcare decisions and data usage. The following principles guide the project's approach to autonomy:

Empowerment: Providing patients with the tools and knowledge needed to make informed decisions about their care and data sharing. This includes clear communication about their rights and the implications of their choices.

Control Over Data: Patients have the right to access, modify, or delete their data. TREAT ensures that mechanisms are in place to respect these rights while maintaining compliance with legal frameworks such as GDPR.

Decision-Making Support: Through personalized recommendations and transparent AI-driven insights, TREAT supports patients in making autonomous decisions regarding their treatments, without overriding their preferences or values.

Minimization of Intrusiveness: The project ensures that any data collection or intervention respects the personal space and dignity of patients, avoiding unnecessary invasiveness.

By addressing these aspects, the TREAT project aligns with high ethical standards, ensuring that patients' rights, dignity, and autonomy are prioritized throughout its implementation.

4. Legal Framework

4.1 Spain

4.1.1 General Data Protection Regulation (GDPR)

The GDPR (General Data Protection Regulation) is a European Union law that regulates the protection of personal data and the privacy of EU citizens. It came into force on May 25, 2018, and sets strict guidelines on how organizations must collect, store, process, and protect personal data.

Key aspects of the GDPR:

- **Clear and explicit consent:** Organizations must obtain explicit and clear consent from individuals to collect and process their personal data.
- **Right of access:** Individuals have the right to know what data is being collected about them, how it is used, and how long it will be retained.
- **Right to be forgotten** Individuals can request that their personal data be deleted when it is no longer needed or if they withdraw their consent.
- **Data portability:** Users can request a copy of their personal data in a structured and transferable format.
- **Data protection by design and by default:** Organizations must implement security and privacy measures at all stages of data processing.
- **Data breach notification:** In the event of a data breach, organizations are required to notify the authorities and affected parties within 72 hours.
- **Severe fines:** Organizations that fail to comply with the GDPR can face significant fines, which can reach up to 4% of global annual revenue or €20 million, whichever is greater.

The main goal of the GDPR is to give citizens and residents control over their personal data and to simplify the regulatory environment for international business by unifying regulation within the EU.

The EU has substantially expanded the definition of personal data under the GDPR. To reflect the types of data organizations now collect about individuals, online identifiers such as IP addresses are now considered personal data. Other data, such as economic, cultural, or mental health information, are also considered personally identifiable information.

Pseudonymous personal data may also be subject to GDPR rules, depending on how easy or difficult it is to identify what the data is.

Anything that was considered personal data under the Data Protection Act also qualifies as personal data under the GDPR.

The first step in ensuring compliance with the GDPR is to understand it. To do this, you must understand the implications of not meeting the required standards.

In order to assess whether these standards are being met, audits must be conducted.

Although this process is different for each company, below are some of the general steps that must be followed to comply with GDPR.

• Understand the GDPR legal framework

The first step to ensuring compliance is to understand the legislation in place, as well as the implications of not meeting the required standards, by conducting a compliance audit against the GDPR legal framework.

• Create a data register

Once companies have a clearer idea of their readiness to comply with regulatory requirements, they should keep a record of the process. This should be done through maintaining a Data Register – essentially a GDPR diary. Each country has a Data Protection Association (DPA), which will be responsible for enforcing the GDPR.

It is this organisation that will judge whether a company has been compliant in determining potential penalties for non-compliance. If a breach occurs during the initial implementation phase, the company should be able to show the DPA its progress towards compliance through its Data Register.

• Classify the data

This step is about understanding what data companies need to protect and how it is being done. First, companies need to find personally identifiable information (PII) – information that can identify someone directly or indirectly – from EU citizens. It's important to identify where it's stored, who has access to it, who it's shared with, etc.

They can then determine what data is most vital to protect, based on its classification. This also means knowing who is responsible for controlling and processing the data, and making sure all the right contracts are in place.

• Start with the top priority

Once the data has been identified, it's important to start assessing the data, including how it's being produced and protected. With any data or application, the first priority should be protecting user privacy. When looking at most private data or applications, companies should always ask themselves if they really need that information and why.

Businesses should complete a Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) of all security policies, assessing the lifecycles of data from source to destruction.

From here, businesses should assess their data protection strategies – how exactly they are protecting data (for example, with encryption, tokenisation or pseudonymization).

• Assess and document additional risks and processes

Aside from the most sensitive data, the next stage is to assess and document other risks, with the aim of finding out where the business may be most vulnerable during other processes.

It is vital for businesses to maintain a roadmap document to show the DPA how and when they are going to address these outstanding risks. It is these actions that show the DPA that the business is taking compliance and data protection seriously.

• Review and repeat

The final step is to review the outcome of the previous steps and remediate any potential deletions, modifications and updates where necessary. Once this is completed, companies should determine their next priorities and repeat the process from step four.

How to apply GDPR in TREAT

In the TREAT project, the GDPR (General Data Protection Regulation) must be applied to ensure that the handling of patients' personal data, including medical and health data, complies with EU privacy regulations. Since the project involves the collection, processing and transmission of sensitive information through technologies such as artificial intelligence, wearables, and semantic interoperability platforms, it is crucial that the GDPR is respected in all phases of the project.

Key GDPR Applications in TREAT

- **Explicit patient consent:**

Before any health data is collected, patients must give their explicit and informed consent. The project must ensure that users understand what data is being collected, how it will be used, and for how long it will be stored.

In addition, consent mechanisms must be easily accessible, with the possibility of revoking consent at any time.

- **Right of access and data portability:**

Patients have the right to access their data at any time and to know how it is being used within TREAT. The possibility of portability of data to other systems or providers should also be offered, if requested.

TREAT must develop a platform that allows users to view and download their information in a clear and secure manner.

- **Data protection by design and by default:**

TREAT's platform and all associated technologies must implement security and privacy measures by design, ensuring that data collection and processing are the minimum necessary (data minimization) and that data is protected by default.

Sensitive data, such as medical records, should be encrypted and anonymized to prevent risks in the event of a security breach.

- **Notification of security breaches:**

If a security breach occurs that affects patients' personal data, TREAT must notify the relevant data protection authorities and those affected within 72 hours.

The project must have a well-defined incident response plan to manage any potential security breach.

- **Data Protection Impact Assessment (DPIA):**

Since TREAT handles sensitive personal data (health data), a Data Protection Impact Assessment (DPIA) must be conducted to identify and mitigate potential risks associated with the processing of this data.

This assessment should include measures to ensure data security, minimize privacy breach risks, and ensure compliance with the GDPR.

- **Anonymisation and pseudonymisation:**

Where possible, data should be anonymised or pseudonymised to reduce the risk of patients being identified from their personal data.

This is especially important in TREAT, where medical data may be shared between different platforms and actors for analysis and recommendation generation.

- **Right to be forgotten:**

Patients can request that their personal data be deleted from the system when it is no longer necessary for the purposes for which it was collected, or if they wish to withdraw their consent.

TREAT should have clear mechanisms in place to process and execute these requests quickly and effectively.

4.1.2 Organic Law on Data Protection and Guarantee of Digital Rights (LOPDGDD)

This law complements the GDPR in Spain, incorporating specific provisions adapted to the Spanish legal framework. It was published in December 2018 and establishes additional rights and specific obligations for companies that process personal data.

TREAT must ensure that it complies with both the GDPR and the LOPDGDD. This includes aspects such as guaranteeing patients' digital rights, establishing clear contracts with service providers (third parties) and adopting appropriate measures for the processing of sensitive data.

Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD) is a Spanish law that complements the General Data Protection Regulation (GDPR) in Spain. Its main objective is to regulate the rights and freedoms of natural persons in relation to the processing of their personal data, as well as to guarantee the protection of citizens' digital rights in the digital environment.

It came into force on December 7, 2018 and expands some provisions of the GDPR, adapting the European regulatory framework to the particularities of the Spanish legal and administrative system.

Main Aspects of the LOPDGDD

- **Consent and Data Processing**

The LOPDGDD reinforces the need to obtain explicit consent for the processing of personal data, especially when handling sensitive data such as health data. In this case, consent must be informed, clear and revocable at any time.

- **Protection of Digital Rights**

The LOPDGDD includes a set of digital rights that address issues such as privacy in the digital sphere, protection of reputation and security of electronic communications.

These rights include:

- Right to be forgotten: Individuals can request the deletion of their personal data if it is no longer necessary for the original purpose of collection.
- Right of access: Individuals can request access to the information that organizations have about them.
- Right to data portability: Users have the right to receive their data in a structured and transferable format.

- **Regulation of Data Processors**

The law requires that organisations that handle personal data, including those that subcontract services related to data processing (such as software companies), enter into contracts with data processors that include clear obligations regarding the handling of personal data.

- **Security Measures**

The LOPDGDD reinforces the obligation to implement appropriate technical and organisational measures to ensure the security of personal data and protect it against unauthorised access, loss, destruction or damage.

- **Data Protection Impact Assessment (DPIA)**

The LOPDGDD requires a Data Protection Impact Assessment (DPIA) to be carried out on projects that involve the processing of sensitive data or that may represent a high risk to the rights and freedoms of individuals.

- **Security Breach Management**

In the event of a security breach affecting personal data, the LOPDGDD requires notification to the Spanish Data Protection Agency (AEPD) within 72 hours and, if necessary, inform affected users.

- **Right to Privacy in the Workplace**

The LOPDGDD introduces specific provisions to protect employee privacy, such as prohibiting excessive monitoring of employee communications and activities without appropriate consent.

Application of the LOPDGDD in the TREAT Project

In the context of TREAT, the LOPDGDD would be applied in the following keyways:

- **Patients' Informed Consent:** Before collecting any health data, TREAT must obtain explicit consent from patients. This consent must include clear information on how their data will be used, with whom it will be shared, and how they can revoke consent.

- **Implementation of Digital Rights:** TREAT must ensure that patients have access to their rights, such as the right to be forgotten and the right of access. This implies that TREAT's platform or digital tools must have interfaces that allow patients to manage their own data effectively.

- **Security Measures and Data Management:** TREAT will need to implement strong security measures, such as encryption and anonymization, to ensure the protection of sensitive patient data. In the event of a security breach, TREAT must notify the relevant authorities and affected patients.

- **Data Protection Impact Assessment:** As TREAT handles sensitive health data, it is essential that a DPIA is carried out to identify and mitigate privacy-related risks. This assessment will help TREAT comply with legal obligations and protect patient rights.

- **Contracts with Data Processors:** If TREAT subcontracts third parties for data processing, such as software developers or platform providers, contracts must be established to ensure that these entities comply with the LOPDGDD and GDPR regulations.

4.1.3 Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a process that helps identify and minimise the privacy risks to personal data before an organisation starts processing data. This assessment is a requirement under the General Data Protection Regulation (GDPR) when the processing of personal data, especially sensitive data such as health data, could pose a high risk to the rights and freedoms of individuals.

Objectives of a DPIA:

- **Identify privacy risks:** Assess how the processing of personal data could affect the privacy and security of individuals.
- **Mitigate those risks:** Propose technical and organizational measures to reduce or eliminate the identified risks.
- **Comply with the GDPR:** Ensure that the project or process complies with the legal obligations of the GDPR.

When is a DPIA necessary?

A DPIA is mandatory when carrying out activities that involve the processing of sensitive data, such as:

- Processing large amounts of health data.
- Using new technologies, such as artificial intelligence, to analyse personal data.
- Systematic monitoring of individuals.

DPIA Application in TREAT Project

The TREAT project, which involves the processing of sensitive medical data through wearable devices, artificial intelligence, semantic interoperability and other advanced technologies, must perform a DPIA to comply with the GDPR and ensure that patients' health data is processed ethically and securely. Here's how DPIA can be applied in TREAT:

- **Identifying risks in the processing of health data:**

Collected data: TREAT collects large amounts of sensitive data, such as medical, biometric and behavioural information from patients, through wearable devices and digital platforms.

Potential risks: Security breaches, unauthorised access, misuse of medical information, lack of transparency on how data is used, etc.

The DPIA must identify these risks and their potential impacts on patients' rights and freedoms.

- **Necessity and proportionality assessment:**

Purpose of processing: The DPIA must analyse whether the collection of health data is strictly necessary for the objectives of the project and whether the data collected is the minimum required for those purposes (data minimization principle).

Adequacy of security measures: The assessment must also consider whether security and privacy measures have been implemented by design (privacy by design) to protect the data.

- **Risk mitigation:**

Technical measures: Data encryption, anonymization or pseudonymization of personal information, limited access control to authorized personnel, among others.

Organizational measures: Staff training in data protection, contracts with third parties that ensure compliance with the GDPR, procedures to handle data breaches.

If risks are identified that cannot be adequately mitigated, the DPIA could recommend re-evaluating the processing of certain data or even stopping its collection.

- **Transparency and informed consent:**

The DPIA must ensure that patients are fully informed about how their data is processed, for what purposes, and who will have access to it. This means that informed consent must be explicit, clear, and easily revocable at any time.

- **Notification to data protection authorities:**

If the DPIA identifies a high risk that cannot be adequately mitigated, the project must notify the data protection authority before proceeding with processing. This will allow the authority to monitor and provide guidance.

- **Ongoing review of the DPIA:**

The DPIA is not a one-time process. As the TREAT project evolves, new technologies are implemented, or the way data is processed changes, it is crucial to review and update the DPIA to ensure continued compliance with the GDPR.

Below is a table of risks initially identified in the TREAT project based on the principles of the DPIA (Data Protection Impact Assessment):

Risk	Description	Impact	Probability	Mitigation Measures
Unauthorized access to sensitive health data	Possibility of unauthorized personnel accessing patients' medical data.	High	Possible	Access controls, multi-factor authentication, and data encryption.
Lack of transparency in data usage	Patients may not be fully informed about how their health data is used and shared.	Medium	Possible	Improve informed consent mechanisms.
Privacy violation due to inadequate anonymization	Risk that personal data could be identifiable due to inadequate anonymization or pseudonymization.	High	Likely	Anonymization and pseudonymization of personal data.
Data transfer risks between platforms	Interoperability between systems may create vulnerabilities during data transfers.	High	Possible	Use of encrypted connections and secure protocols.
Non-compliance with the right to be forgotten	Difficulty ensuring that patients' personal data can be fully deleted upon request.	Medium	Possible	Implement automated processes for data deletion upon request.
Unnecessary retention of data	Storing personal data longer than necessary increases the risk of data breaches.	Medium	Possible	Establish clear data retention policies.
Misuse of data by third parties	Potential misuse or sharing of data by third parties with access to TREAT systems.	High	Possible	Strict contractual agreements and regular audits with third parties.
Security breach risk	Security breaches compromising the confidentiality and integrity of patients' medical data.	High	Likely	Constant monitoring, firewalls, and intrusion detection systems.
Use of AI without clear explainability	AI may provide recommendations without proper explanation, impacting patient trust.	Medium	Possible	Develop explainable and transparent AI models.
Non-compliance with GDPR in new updates	Risk that new functions or technologies implemented may not comply with GDPR requirements.	Medium	Possible	Regular DPIA reviews and legal audits.

Explanation of the columns:

- **Risk:** Identifies the specific risk related to the processing of personal data in the TREAT project.
- **Description:** Explains the potential risk in detail.

- **Impact:** Measures the severity of the risk in terms of the impact it could have on the project or on the privacy of patients (Low, Medium, High).
- **Probability:** The possibility of the risk occurring (Rare, Possible, Likely, Almost Certain).
- **Mitigation Measures:** Actions that are or will be taken to reduce or eliminate the risk.
- **Responsible:** The team or person in charge of implementing the mitigation measures.
- **Status:** The current phase of risk management (Identifying, Mitigating, Monitoring).

This risk table is a fundamental tool to ensure that the TREAT project handles data securely and in compliance with regulations such as the GDPR, while protecting the privacy and rights of patients.

4.2 Portugal

General Data Protection Regulation (GDPR)

The GDPR (General Data Protection Regulation) is a European Union law that regulates the protection of personal data and the privacy of EU citizens. It came into force on May 25, 2018, and sets strict guidelines on how organizations must collect, store, process, and protect personal data.

The Portuguese data privacy law (Law No. 58/2019 of 8 August 2019) repealed the former data privacy law and executed Regulation (EU) 679/2016 on General Data Protection Regulation (GDPR).

In this project, synthetic data are used for the development and testing of the application, ensuring that no real patient data are involved. During clinical practice, when the application is employed, access to patient data is restricted to the healthcare professionals responsible for the patient's care, and all performance indicators and clinical supervision data are anonymized.

- **Technical and Organizational Measures and Data Processing Security**

The project should describe the data sources to be used in the production environment for developing digital tools that support patients and their families. It should detail the measures that ensure correct compliance with the organization's policies and practices in light of the obligations under the data protection regulations.

All data sources necessary to integrate the clinical systems being developed must be described. Appropriate and necessary technical and organizational measures must be adopted to ensure and demonstrate that all data processing activities within the application scope comply with the GDPR from the moment of its implementation.

- **Data Protection by Design and Impact Assessment**

You should rigorously evaluate the types of data processing you plan to carry out in the near future. This involves analyzing their nature and context, as well as the potential risks they may pose to data subjects, to effectively apply the principles of data protection by design and by default.

The GDPR expressly requires the adoption of data protection measures at the time of determining the means of processing and during the data processing itself, so timely application should be considered. In the context of processing clinical data in a production environment, if the processing is likely to result in a high risk, a Data Protection Impact Assessment (DPIA) should be conducted to adopt appropriate measures to mitigate those risks.

- **Notification of Security Breaches**

Establish procedures for handling personal data breaches, including the detection, identification, and investigation of incidents; implementing mitigating measures; managing information flows between the data controller and processor; involving the Data Protection Officer; and notifying the National Data Protection Commission (CNPD), in accordance with the timeframes prescribed in the regulation.

Not all breaches need to be reported to the supervisory authority—only those likely to result in a risk to the rights of data subjects. However, all breaches must be properly documented as stipulated in the regulation.

4.2.1 General Data Protection Regulation (GDPR) and Portuguese National Law in the Healthcare Sector

The General Data Protection Regulation (GDPR) is a European Union regulation that governs the protection of personal data and the privacy of individuals within the EU. It came into effect on May 25, 2018, setting stringent guidelines on how organizations must collect, store, process, and protect personal data.

In Portugal, the GDPR is supplemented by national legislation, particularly Law No. 58/2019 of August 8, which implements the GDPR within the Portuguese legal framework. In the healthcare sector, additional specific regulations apply due to the sensitive nature of health data.

Key Aspects of the GDPR and Portuguese Law in the Healthcare Sector

- **Clear and Explicit Consent:** Organizations must obtain explicit and informed consent from individuals to collect and process their personal and health data. In healthcare, consent must be specific and based on clear information about the purposes of data processing. However, processing may be lawful without consent if necessary for medical diagnosis, provision of health or social care, or treatment under professional secrecy.
- **Lawful Processing of Health Data:** Health data is classified as a special category of personal data requiring enhanced protection. Processing is permitted under specific conditions, such as when necessary for preventive or occupational medicine, medical diagnosis, or the provision of health or social care.
- **Right of Access:** Individuals have the right to access their personal data, including medical records, and to know how their data is used, who it is shared with, and how long it will be retained.
- **Right to Rectification and Erasure:** Individuals can request the correction of inaccurate personal data and, under certain conditions, request the deletion of their data ("right to be forgotten"). In healthcare, data may need to be retained to comply with legal obligations or for public health interests.
- **Data Portability:** Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller.
- **Data Protection by Design and by Default:** Organizations must implement appropriate technical and organizational measures to ensure data protection principles are integrated into processing activities, especially in systems handling health data.
- **Data Breach Notification:** In the event of a personal data breach, organizations must notify the competent supervisory authority—the National Data Protection Commission (Comissão Nacional de Proteção de Dados, CNPD)—within 72 hours. If the breach poses a high risk to individuals' rights and freedoms, affected individuals must also be informed without undue delay.
- **Appointment of a Data Protection Officer (DPO):** Organizations that process special categories of data on a large scale, such as hospitals and healthcare providers, are required to appoint a DPO to oversee compliance with data protection laws.
- **Severe Fines:** Non-compliance with the GDPR and Portuguese data protection laws can result in significant fines, up to 4% of the global annual turnover or €20 million, whichever is greater.

4.2.2 Data Protection by Design, Privacy Impact Assessments, and Data Protection Impact Assessments

Organizations, particularly in the healthcare sector, must rigorously evaluate the types of data processing activities they plan to undertake. This involves analyzing the nature, scope, context, and purposes of processing, as well as the potential risks to data subjects.

- **Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA):** Businesses should complete both a Privacy Impact Assessment (PIA) and a Data Protection Impact Assessment (DPIA) for all security policies. These assessments involve evaluating the entire lifecycle of data—from collection to destruction—to identify and mitigate potential risks to personal data.
    - **Assessing Data Lifecycles:** The assessments should cover how data is collected, stored, accessed, used, shared, and ultimately destroyed or archived. This comprehensive evaluation ensures that data protection principles are embedded throughout the data lifecycle.
    - **Implementing Mitigation Measures:** Based on the findings of the PIA and DPIA, organizations should implement appropriate technical and organizational measures to address identified risks. This may include data minimization, pseudonymization, encryption, access controls, and regular security testing.

GDPR expressly requires the adoption of data protection measures both at the time of determining the means of processing and during the processing itself. Timely and proactive application of these measures is crucial.

In the context of processing clinical data in a production environment, conducting PIAs and DPIAs is essential due to the high risks associated with handling sensitive health data. These assessments help organizations comply with the principles of data protection by design and by default.

Notification of Security Breaches

Establish procedures for handling personal data breaches, including:

- **Detection and Identification:** Promptly identify and investigate incidents involving personal data breaches.
- **Mitigation Measures:** Implement measures to contain and mitigate the effects of the breach.
- **Information Flows:** Manage communication between the data controller and processor, ensuring all parties are informed and actions are coordinated.
- **Involvement of the Data Protection Officer (DPO):** The DPO should be actively involved in managing the breach response.
- **Notification to CNPD:** Notify the National Data Protection Commission (CNPD) within 72 hours, as prescribed by the regulation, if the breach is likely to result in a risk to individuals' rights and freedoms.

Not all breaches need to be reported to the supervisory authority—only those likely to result in a risk to the rights of data subjects. However, all breaches must be properly documented as stipulated in the regulation.

Definition of Personal Data

Under the GDPR, personal data includes any information relating to an identified or identifiable natural person. This encompasses a wide range of identifiers, such as:

- **Direct Identifiers:** Names, identification numbers, and location data.
- **Online Identifiers:** IP addresses and cookies.
- **Special Categories of Data:** Health information, genetic data, biometric data, and data revealing racial or ethnic origin, political opinions, religious beliefs, or sexual orientation.

The EU has substantially expanded the definition of personal data under the GDPR to reflect the types of data organizations now collect. In the healthcare sector, this means that all patient-related information is subject to strict data protection requirements.

Special Considerations in the Portuguese Healthcare Sector

- **Professional Confidentiality Obligations:** Healthcare professionals are bound by strict confidentiality obligations under Law No. 12/2005 and professional codes of ethics. Unauthorized disclosure of patient data can lead to disciplinary actions and legal consequences.
- **Electronic Health Records (EHR):** Decree-Law No. 18/2017 regulates the use of electronic health records, emphasizing data security, interoperability, and patient confidentiality. Healthcare providers must ensure that EHR systems comply with data protection requirements.

Data Retention Periods: Portuguese law establishes minimum retention periods for medical records (typically 20 years after the last entry), which must be observed even if individuals request data deletion, provided retention is necessary for legal compliance.

Ensuring Compliance

- **Understanding Legal Obligations:** Healthcare organizations must thoroughly understand the GDPR and relevant Portuguese laws to ensure compliance when processing health data. This includes recognizing the implications of non-compliance, such as severe fines and reputational damage.
- **Conducting Audits:** Regular audits should be performed to assess whether data protection standards are being met. This involves reviewing data processing activities, security measures, and compliance with policies and procedures.
- **Implementing Security Measures:** Adopt appropriate technical and organizational measures to ensure data security, including encryption, access controls, and regular security assessments.
- **Staff Training and Awareness:** Regular training programs should be conducted to ensure all staff members understand their responsibilities regarding data protection and confidentiality.
- **Appointment of a Data Protection Officer (DPO):** Designate a DPO responsible for overseeing data protection strategies and ensuring compliance with legal requirements.

In the TREAT project, strict adherence to the General Data Protection Regulation (GDPR) and Portuguese national data protection laws is essential to ensure that the handling of patients' personal and medical data complies with EU and national privacy regulations. The project involves the collection, processing, and

transmission of sensitive health information using technologies such as artificial intelligence, wearable devices, and semantic interoperability platforms.

Use of Synthetic Data and Anonymization

- **Development Phase:** During the development process, synthetic data are used instead of real patient data. This approach eliminates the risk of exposing personal health information and simplifies compliance with data protection laws during this phase.
- **Production Phase:** In the production environment, access to data is anonymized, and only clinical indicators are utilized. Personal identifiers are removed or masked to prevent the re-identification of individuals. This ensures that while useful clinical data are available for healthcare purposes, patient privacy is maintained.

4.2.3 Simplified Risk Assessment Based on DPIA Principles

Despite these measures, it's important to conduct a Data Protection Impact Assessment (DPIA) to identify and mitigate any potential risks associated with data processing. Below is a simplified overview of the risks initially identified in the TREAT project, adapted to comply with GDPR and Portuguese law:

Potential Risk	**Description**	**Mitigation Measures**	**Impact**
Unauthorized Access to Data	Risk that unauthorized individuals could access sensitive health data, even if anonymized.	- Implement strict access controls and multi-factor authentication mechanisms. - Regularly update and audit user access rights. - Use secure channels for data encryption.	High
Re-identification of Anonymized Data	Possibility that anonymized data could be re-identified by combining with other data sources.	- Apply robust anonymization and pseudonymization techniques. - Limit the amount of data shared and ensure it's the minimum necessary. - Monitor and control data linking activities.	Medium
Data Breach or Security Incident	Risk of data loss or exposure due to cyber-attacks or system failures.	- Implement strong encryption for data at rest and in transit. - Establish incident response and data breach notification procedures. - Conduct regular security assessments and penetration testing.	High
Non-compliance with GDPR and National Laws	Failure to adhere to legal obligations could result in fines and legal action.	- Stay updated with GDPR and Portuguese data protection laws. - Appoint a Data Protection Officer (DPO) to oversee compliance.	High

		- Provide regular staff training on data protection practices.	
Third-Party Risks	Risks arising from third-party service providers who have access to the data.	- Ensure all third parties are compliant with GDPR and Portuguese laws. - Include data protection clauses in all contracts. - Conduct due diligence and regular audits of third-party practices.	Medium
Inadequate Data Destruction Practices	Risk that data is not properly deleted, leading to potential unauthorized access.	- Establish clear data retention and deletion policies. - Use secure data destruction methods. - Regularly review and purge data that is no longer necessary.	Medium

Using synthetic data during development and ensuring data is anonymized in the production phase with access limited to clinical indicators, the TREAT project significantly reduces the risks associated with handling personal health data. However, it's crucial to remain vigilant and proactive:

- **Conduct a DPIA:** Even with minimized risks, performing a DPIA is essential to systematically analyze data processing activities and implement appropriate safeguards.
- **Ensure Ongoing Compliance:** Continuously monitor and update data protection measures to stay aligned with GDPR and Portuguese legal requirements.
- **Educate and Train Staff:** Regular training sessions should be held to keep all team members informed about data protection obligations and best practices.
- **To design and implement an education plan** that ensures all professionals and staff involved in the TREAT project are knowledgeable about data protection obligations and best practices, in compliance with the GDPR and Portuguese data protection laws within the healthcare sector.

4.3 Türkiye

4.3.1 Data Security and Privacy Requirements

In this use case, patient groups with diabetics are included in the study. The data that are taken from these patient groups from both Patient history data from Anadolu Sigorta and health data to be collected from Livewell's wearable clothes. Before the data collection begins from related patients, these patients are informed due to KVKK rules and ethical approval.

✓ All communication and data storage must be end-to-end encrypted to prevent unauthorized access to medical information.

✓ Restrict access to authorized personnel only and verify user identities.

✓ The data is processed within the individual software components on researcher computers.

✓ The imaging data must be systematically anonymized.

✓ Before the data collection begins, the test persons are informed comprehensively and must sign an informed consent.

✓ The dataset is not to be shared with other parties or companies not actively collaborating in the same research.

4.3.2 Legal and Ethical Requirements

To ensure strict adherence to Turkey's Personal Data Protection Law (KVKK) and to safeguard the rights of the participants, the project will diligently seek and obtain approval from the ethics committee. Maintaining full compliance with KVKK regulations is of paramount importance to secure the confidentiality of participant data.

✓ University Ethics Committee approval number must be obtained before the data collection begins. The research received specific grant from funding agency must be introduced to Ethical Committee.

✓ Informed and voluntary consent must be obtained from all subjects before data collection begins.

✓ Researcher must declare that they have no known competing financial interests or personal relationship that could have appeared to influence the data collection.

4.3.3 Standards and Regulations

✓ Subjects have the right to request information about their stored personal and medical data, request corrections, receive a free copy, and pass this data on to other responsible parties.

✓ If subjects doubt the accuracy of their stored data, have objected to the data processing, or the data processing is unlawful, they have the right to request a restriction of the processing of the data.

✓ The imaging data must be systematically reviewed and categorized to groups.

4.3.4 Data Protection Requirements

✓ Comprehensive anonymization and de-identification techniques are essential to minimize the risk of re-identification and protect the identities of individuals within the imaging dataset.

✓ All patient data will be encrypted to prevent unauthorized access. Encryption protocols will comply with relevant data protection laws.

✓ Subjects have the right to request information about their personal data stored at any time.

✓ Informed and voluntary consent can be withdrawn at any time and contact forms for full data and images of patients' deletion requests will be provided.

4.3.5 Data Storage Requirements

✓ The patient and its historical data will be stored exclusively on local storage systems and will be protected from unauthorized access within the framework of access control to the premises of the participating research partners. Data sharing has been limited to collaborators within the project.

✓ In case of informed consent open access data publication, all data will be completely anonymized.

✓ After study completion, anonymized data will be stored for at least 5 years in line with local law.

✓ Access to patient data will be strictly controlled and limited to authorized personnel through role-based access controls.

4.3.6 Data Re-use Opportunity

The data will be used in anonymized form in open scientific research. Anonymized data can be valuable for research and analysis on monitoring diabetic and heart disease patient. The valuable results of this research can be published in articles and journals as part of open science practices.

4.4 Canada

4.4.1 Personal Information Protection and Electronic Documents Act (PIPEDA)

The Personal Information Protection and Electronic Documents Act, PIPEDA, is the primary law which regulates how personal information is collected, used and disclosed in Canada. PIPEDA rules to govern the collection, use and disclosure of personal data (defined as personal information under the law) in a manner that recognizes the right of privacy of individuals with respect to their personal data and the need of organizations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. It applies to every organization that collects, uses, or discloses personal data in the course of commercial activities.

PIPEDA requires compliance with 10 Fair Information Principles and includes guidance on requirements for protection of personal data, breaches of security safeguards, complaints, investigations and remedies as carried out by the Office of the Privacy Commissioner of Canada.

The PIPEDA 10 Fair Information Principles are:

1. **Accountability**: An organization is responsible for personal data under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. **Identifying Purposes**: The purposes for which personal data is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent**: The knowledge and consent of the individual are required for the collection, use or disclosure of personal data, except when inappropriate.

4. **Limiting Collection**: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention**: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfilment of those purposes.

6. **Accuracy**: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness**: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. **Individual Access**: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance**: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Key PIPEDA Applications in TREAT

TREAT will clearly outline the objectives for collecting personal data, which include monitoring health metrics, delivering personalized feedback, and enhancing communication between patients and clinicians. Patients will be informed about the data collected through wearable devices and digital platforms. Their understanding and consent will be secured prior to any data collection, ensuring that they are fully aware of how their information will be utilized.

The data gathered will be strictly confined to what is necessary for the specified purposes, such as activity data and other pertinent health metrics. Personal data will be utilized solely for the reasons for which it was collected, including improving patient care and enabling real-time decision-making. Additionally, data retention will occur only for as long as necessary to fulfill these purposes.

The system will be designed to guarantee that personal information collected is accurate, complete, and current while also safeguarding sensitive data from unauthorized access. They will be provided with clear information about the policies and practices regarding the management of personal information, recognizing that they have the right to access their collected personal information and to raise any concerns regarding adherence to PIPEDA principles.

4.4.2 3.4.2 PIPEDA Adequacy under the GDPR and Data Residency

As of January 2024, the European Commission has found Canada continues to provide an adequate level of protection of personal data transferred from the European Union to recipients that are subject to PIPEDA. This decision means that personal data can be transferred from the European Union to Canada without specific authorization, as stated in GDPR Article 45.

PIPEDA itself has no restrictions on the transfer of data between Canada and the European Union or other third parties. In Canada, only two provinces, British Columbia and Nova Scotia, have restrictions on personal data transfer outside the country; in both cases, restrictions apply only when processing personal data on behalf of provincial public-sector entities/ operations. However, other provinces substantially similar to PIPEDA (Alberta, Quebec) require transparency on international data processing

4.4.3 Substantially Similar to PIPEDA

PIPEDA in Canada is the primary privacy legislation for commercial organizations; however there in an exception where substantially similar legislation exists at the provincial level. Substantially similar legislation exists in Alberta (the Personal Information Protection Act of Alberta, PIPA AB), British Columbia (the Personal Information Protection Act of British Columbia, PIPA BC) and Quebec (the Act Respecting the Protection of Personal Information in the Private Sector, ARPPIPS).

4.4.4 Personal Health Information Privacy in Canada

In some provinces and territories, Canada has legislation dealing specifically with health information protection. The following is a list of health privacy legislations that may apply to TREAT's collection, use, processing, retention and disclosure of personal data that includes health information in Canada:

- Alberta - Health Information Act (HIA)
- Manitoba - Personal Health Information Act (PHIA)
- New Brunswick - Personal Health Information Privacy and Access Act (PHIPA)
- Newfoundland and Labrador - Personal Health Information Act (PHIA)
- Nova Scotia - Personal Health Information Act (PHIA)
- Northwest Territories - Health Information Act (HIA)
- Nunavut - Access to Information and Protection of Privacy Act (ATIPP)
- Ontario - Personal Health Information Protection Act (PHIPA)
- Prince Edward Island - Health Information Act (HIA)
- Québec – Act Respecting Health and Social Service Information (ARHSSI)
- Saskatchewan - Health Information Protection Act (HIPA)
- Yukon - Health Information Privacy and Management Act (HIPMA)

4.4.5 Public Sector Privacy in Canada

If public entities are involved with the TREAT Project, the Privacy Act of Canada (Federal) or Provincial Privacy Acts may need to be considered. If working with a hospital in British Columbia for example, FIPPA often applies where British Columbia does not have a separate law for health information but does have laws for provincial bodies and provincially funded institutions.

4.4.6 The Artificial Intelligence and Data Act

In June 2022, the Government of Canada tabled the Artificial Intelligence and Data Act as part of Bill C-27. The law is intended to establish common requirements across Canada for the design, development and use of AI systems, and prohibit conduct that may result in serious harm to individuals or harm to their interests. As of October 2024, the bill has yet to pass into law. However, where the TREAT project intends to use artificial intelligence, attention on the bill will be needed if it passes, including any new requirements and when the law goes into effect.

4.4.7 Access to Health Records for ML/AI training

For the Canada use case, Rehabtronics will obtain anonymized patient medical record data from Providence Health Care (PHC) to develop a model for predicting pressure injuries and ulcers. A Clinical Collaborative Research Agreement will govern the data usage and research, ensuring compliance with

privacy laws such as PIPEDA and HIPAA. Additionally, the PHC Internal Review Board (IRB) must approve the data's use for generating the ML/AI model.

4.4.8 General Steps to Comply with Canadian Privacy Law

Where different privacy laws may apply, below are some of the general steps that assist in compliance with Canadian requirements.

1. **Determine the data subjects' residency and who is invested in the project to confirm what laws apply**

The first step to ensuring compliance is to understand what privacy laws apply. This is determined by:

- Establish where the personal data is coming from, or where there will be a high likelihood of participants. If deliberately collecting data from residents of Quebec, compliance with ARPPIPS is advised, which will include a Privacy Impact Assessment on data leaving the province. If collecting information from British Columbia, confirm the requirements of PIPA BC are being met.

- Who is invested in the project? If personal data is being collected, used, accessed, processed or retained by or on behalf of registered healthcare practitioners, clinics, hospitals and/ or licenced healthcare providers, likely provincial health privacy laws apply. If personal data is being collected, used, accessed, processed or retained by public sector entities, or if public bodies are funding the project, they may have contractual requirements as part of data sharing agreements that issue TREAT must comply with applicable public sector legislation.

2. **Confirm compliance with the 10 Fair Information Principles**

While legislations differ, the 10 Fair Information Principles of PIPEDA are common aspects of all Canadian privacy laws. Compliance with the 10 Fair Information Principles confirms compliance with majority of provincial health and public sector legislation.

- Assign an individual, such as a Privacy Officer, Chief Privacy Officer or Chief Privacy and Security Officer, who is responsible to confirm adequate policies and privacy protection practices are in place.

- Require agreements with partners before the collection, processing, use, retention or disclosure of personal data, including contracts with suppliers who require access to personal data, contain provisions to protect personal data.

- Establish written information security and privacy policies that are adhered to for the duration of the project. This should include a policy and procedure for incident management, keeping a record of privacy incidents and breaches with notification to data subjects if the breach involves real risk of significant harm. For health information, multiple health information legislations include requirements to provide reports on access to the data.

- Establish the purpose of personal data collection prior to collection, use or processing.

- Limit collection to data to that what is needed for the purposes identified. Use de-identified, aggregate or anonymized information whenever possible if it will serve the identified purposes.

- Provide a Privacy Policy (Privacy Notice) to inform data subjects, stakeholders and the public of TREAT's privacy practices, including intended data collection, use, and how to exercise data subject rights. If data is de-identified, aggregated or made anonymous as part of the project, inform the data subject.

- Review consent to determine consent is freely given, and the form of consent is adequate for the intended purpose of collection/ use/ disclosure.

- Confirm all individuals with access to personal data sign agreements on privacy protection prior to accessing personal data and receive mandatory privacy and security training.

- Access to personal data must be strictly on a need-to-know basis, as part of the individual's role and responsibilities. For some provincial health privacy legislations, individual data subjects have the right to request specific individuals not have access to their personal data.

- Data subjects have the right to request access or make corrections to their personal data. Requests for access to personal data should be verified to confirm the requestor has legitimate authority to access and not take longer than 30 days to fulfill unless an extension is provided to the requestor.

- If personal data is at the end of its retention period, it must be destroyed in a secure manner.

- Significant administrative, technical and physical security safeguards must be placed to prevent unauthorized collection, access, use or disclosure of personal data. This includes the implementation of workforce controls and disciplinary/corrective action in the event of data misuse.

- Individuals have the right to challenge compliance. A complaints protocol is advised to confirm that all challenges to compliance are recorded and investigated in a timely manner. In the event of non-compliance, rectification action is taken.

- Conduct assessments with assistance from third parties. Privacy Impact Assessments (PIAs) review application of 10 Fair information Principles and compliance with applicable privacy laws. Vulnerability testing and Threat/Risk Assessments should be used to discover and rectify potential security weak points.

3. **Special requirements for Quebec**

In addition to the Fair Information Principles, Quebec's ARPPIPS provides additional data subject rights for residents of Quebec. As these rights are substantially similar to data subject rights in the GDPR, they should be incorporated into TREAT project compliance.

- **Privacy Impact Assessments and data portability:** Any person carrying on an enterprise must conduct a privacy impact assessment for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, communication, keeping or destruction of personal data. The person must also ensure that the project allows computerized personal data collected from the data subject concerned to be communicated to them in a structured, commonly used technological format.

- **Data protection by design and by default:** Any person carrying on an enterprise who collects personal data when offering to the public a technological product or service having privacy settings must ensure that those settings provide the highest level of confidentiality by default, without any intervention by the data subject concerned.

- **Special documentation if data is anonymized as part of the project.** See “Strategies for storing processing and anonymizing participants' personal data” for details.

- **Automated Decision-Making**: Any person carrying on an enterprise who uses personal data to render a decision based exclusively on an automated processing of such information must inform the person concerned accordingly not later than at the time it informs the person of the decision. They must also inform the data subject:
  - (1) of the personal information used to render the decision.
  - (2) of the reasons and the principal factors and parameters that led to the decision; and
  - (3) of the right of the person concerned to have the personal information used to render the decision corrected.

Key Applications in TREAT

Effective handling of patient data within TREAT is critical for ensuring compliance with provincial regulations. To uphold the 10 Fair Information Principles, TREAT will appoint a Privacy Officer responsible for overseeing adherence to privacy policies when managing patient data within their technology. They will collect only the data necessary for their use case and implement strict access controls to safeguard patient information, always ensuring data security and privacy. All patients will receive a comprehensive Privacy Policy that outlines data collection, usage, and their rights regarding personal data. Furthermore, they will conduct regular Privacy Impact Assessments to evaluate compliance with the 10 Fair Information Principles and relevant privacy laws, ensuring the safety of patient data.

When handling personal data of patients residing in Quebec, TREAT policies will also ensure compliance with Quebec's ARPIPS, in addition to the Fair Information Principles. They will incorporate these rights into the compliance framework for the project. Additionally, TREAT will ensure that the privacy settings in their technological products provide the highest level of confidentiality by default. As their use case involves automated processing technology, they will ensure that patients are informed about the technology and understand how their personal data is used.

4.4.9 The Enhancing Digital Security and Trust Act of Ontario

Enacted in November of 2024, the Enhancing Digital Security and Trust Act includes requirements for the use of AI by the public sector in the province of Ontario. Information must be provided to the public on the use of AI solutions. The public sector entity using AI must develop and implement an accountability framework as part of their use of the solution. It must take steps to manage risks associated with AI systems. This Act will apply if TREAT partners with public sector agencies in the province of Ontario.

4.4.10 Privacy Impact Assessment

A Privacy Impact Assessment is an analysis of how personal data is handled to ensure compliance with appropriate regulations. A PIA determines the privacy risks associated with information systems or activities and evaluates ways to reduce the privacy risks. PIAs are substantially similar to DPIAs: a DPIA may substitute for a PIA in Canada, so long as Canadian privacy legislations and regulations are taken into account as part of the analysis.

Below is a simplified overview of the risks initially identified in the TREAT project, based on the ISO/IEC 29134-Guidelines for Privacy Impact Assessment. In addition to the risks below, it is commonplace in

Canadian PIAs to include an analysis of how Personal Data is processed in compliance with the CSA Model Code for the Protection of Personal Information principles, and specific requirements of applicable legislation.

Potential Risk/ Threat	Description	Impact[1]	Sample Mitigation Measures
Unauthorized use or disclosureof Personal Data by internal agent (non-malicious)	Employee or agent of TREAT browses the files of family, friends or VIPs. Employee or agent of TREAT accidentally discloses Personal Data to a third-party. E.g., Loss of mobile device, careless positioning of monitor so that unauthorized persons can view data.	Medium	• Officeror individual accountable for program, policy implementation. • Privacyand security policies.Staff training. • Codeof Conduct. • Limited access toPersonal Data.
Unauthorized use or disclosureof Personal Data by internalagent (deliberate, malicious)	Employee or agent of TREAT deliberately discloses Personal Data to a third-party. E.g., Disgruntledemployee, whistleblower, financial benefit, extortion.	High	• Administrative, technical and physical security measures including backups, encryption, endpoint protection. • Authentication • Security Threat/Risk Assessments, audits. • Eventlogging and monitoring. Auditingof access. • Workforce controls.
Attack by external malicious agent	Hacking, identity theft, social engineering, virus, DDoS	Very High	• Administrative, technicaland physical security measures, including backups, encryption, endpoint protection. • Authentication • Limited access to personal data.

			• Event logging and monitoring. Auditing of access. • Security Threat/Risk Assessments, audits. • Staff training.
Loss of device or improper disposal of media containing Personal Data	Loss or theft of portable device. Paper records, CDs, DVDs and tapes not shredded, portable electronic media, hard drives or other electronic media not degaussed or destroyed before decommissioning.	Medium	• Backups • Limitations on portable devices that may be used for project. • Policies. • Asset inventories. • Classification of portable media. • Encryption of all data at rest.
Accidental corruption of Personal Data	Failure to accurately input Personal Data, errors in automatic feeds.	Low	• Authentication and limited access. • Encryption of data in transit. • Event logs, auditing and monitoring. • Backups to restore to non-corrupted state.
Denial of individual rights	Individual denied access to Personal Data, failure to respect consent directives, no method to challenge compliance.	Medium	• Officer or individual accountable for program. • Policies, processes for individuals to request access to and amendments of Personal Data. • Contracts with all third-party processors. • Data element inventory with purpose of Personal Data,

			limited collection. • Privacy Notice/ Public Privacy Policy • PIA/ DPIA with legislation analysis.

4.4.11 Artificial Intelligence Impact/ Risk Assessments

The purpose of an Artificial Intelligence Impact/Risk Assessment (AIIRA) is to identify risks and mitigation measures to specifically for the management of Artificial Intelligence (AI) systems and implementation. While standards are still in development, with ISO/IEC FDIS 42005 Information technology — Artificial intelligence — AI system impact assessments expected to release in 2025, an AIIRA is not mandatory for the TREAT project to date. However, where the TREAT project will be processing sensitive medical data through artificial intelligence, an AIIRA is advised to show efforts have been taken towards the ethical implementation of AI in the treat project.

Below is a simplified overview of the risks initially identified in the TREAT project. These risks have been identified by material from ISO/IEC: 23894: Information technology – Artificial Intelligence – Guidance on risk management.

Potential Risk/ Threat	Description	Impact[2]	Sample Mitigation Measures
Deepfake technology	Advancements in deepfake technology enable the creation of realistic but fabricated audio, video, or images, which can be used to manipulate public opinion or tarnish individuals' reputations by spreading false information.	High	• AI Detection Systems. • Source Verification. • Policy and Legal Frameworks. • Public Awareness Campaigns. Authentication Protocols.
Algorithmic Bias and Discrimination	Automated decision-making systems powered by algorithms may inadvertently perpetuate biases or discrimination against certain individuals or groups based on factors such as race, gender, or socioeconomic status, compromising privacy and fairness.	Very High	• Bias Detection and Mitigation algorithms, audits. • Diverse Training Data. • Transparency and Explainability (Notice). • Human Oversight. • Accountability Mechanisms. • Fairness and Accuracy Audits.
Lack of Transparency,	When AI systems make decisions impacting	Medium	• Explainability (Notice). • Right to Opt-Out.

including lack of Transparency in AI Decision-Making	individuals without clear explanations or transparency, it can lead to a loss of trust, reduced accountability, and the inability for individuals to understand or challenge outcomes. Failure to explain AI and respect individuals' right to refuse AI decision-making involves not providing clear and transparent explanations about how AI algorithms make decisions and disregarding individuals' autonomy to opt out of or challenge AI-generated decisions that affect them. This failure can lead to distrust, lack of accountability, and potentially harmful impacts on individuals and society.		• Transparency in AI Usage. • Right to Challenge. • Impact Assessments.
Failure to respect consent directives	Organizations must obtain proper consent before using individuals' data for AI or other purposes to avoid breaching privacy and trust. Failure to respect consent directives can lead to legal and ethical implications, violations of data protection regulations, unauthorized profiling, and potential harm to individuals.	Medium	• InformedConsent Frameworks. • Dynamic Consent. • Data Use Notifications. • Audit Trails. • Policies.
Non-compliance with Privacy Legislation and Data Subject Rights	Failure to comply with applicable privacy laws can result in significant penalties, legal actions, and reputational damage. Non-compliance may occur due to improper data handling, unauthorized processing, or inadequate safeguarding measures.	High	• Regular Privacy Audits. • Privacy Awareness Training. • Privacy Officer Oversight. • Record-Keeping Requirements.
Permissible Uses and Secondary Uses	Data collected for one purpose may be used for secondary purposes	Medium	• Purpose Limitation. • Secondary Use Consent. • Data Classification.

of Data. Data Aggregation and Fusion	without user consent, leading to potential privacy violations, unauthorized profiling, or data misuse. Data Aggregation and Fusion: Companies may aggregate and combine data from multiple sources to create comprehensive profiles of individuals, potentially revealing sensitive information or patterns that individuals may not want to disclose.		• Transparency and User Control. • Data Governance Policies. • Privacy Impact Assessments (PIAs)/ Data Protection Impact Assessments (DPIAs).
Artificial Confabulation	A response generated by AI that contains false or misleading information is presented as fact.	High	• Source Verification. • Transparency. • Human Oversight. • Terms of Service and Acceptable Use. • Ongoing Monitoring.
Lack of Due Diligence in AI Vendor Selection	Organizations may fail to perform adequate due diligence when selecting AI vendors, resulting in the use of systems that may not meet privacy standards or legal requirements, potentially leading to privacy breaches or ethical concerns.	Medium	• Vendor Risk Assessments. • Contractual Obligations. • Ethical AI Frameworks. • Data Processing Agreements (DPAs. • Data Transfer Agreements. • Ongoing Monitoring. • Data Ownership Clauses.
Inadequate Safeguarding of Information Assets	Failure to adequately protect information assets, such as databases, files, and networks, from unauthorized access, misuse, or physical theft can result in data breaches, loss of confidentiality, integrity, and availability of sensitive information. This can include personal data, intellectual property, and other critical business information, leading to financial losses, legal penalties, and reputational damage.	High	• Data Encryption. • Access Control Policies. • Data Classification. • Network Segmentation. • Endpoint Security. • BackupandRecovery Plans. • PhysicalSecurity Controls. • SecurityAwareness Training. • Incident Response Plan. • Audit and Monitoring. • Third-Party Vendor Risk Management. • Data LossPrevention (DLP):.

4.5 Netherlands

4.5.1 Introduction

In general, the main legal framework that are applicable in the Netherland within the concept of the TREAT project are the research involving human subjects act (WMO) and the General Data Protection Regulation (GDPR). Another important document that is applicable is the declaration of Helsinki, latest amended during the 64th WMA general assembly in Fortaleza, Brazil (October 2013).

When performing research with medical devices, additional regulations and standards apply. These include the Medical Device Directive (MDR) and ISO 14155: Clinical investigation of medical devices for human subjects – Good clinical practice

In the next sections, these laws will be described in detail.

4.5.2 Research involving human subjects act (WMO)

The main legal framework in the Netherlands that is applicable within the concept of TREAT is the 'Research involving human subjects act' (WMO). The General Data Protection Regulation and, if applicable, the Medical Device Directive are all integrated within the WMO.

Research is subject to the WMO if the following criteria are met:

- It concerns medical scientific research, and
- Participants are subject to procedures or are required to follow rules of behaviour.

There is no clear definition of what medical scientific research is, but Central Committee on Research Involving Human Subjects defines it as:

> "Medical/scientific research is research which is carried out with the aim of finding answers to a question in the field of illness and health (etiology, pathogenesis, signs/symptoms, diagnosis, prevention, outcome or treatment of illness), by systematically collecting and analysing data. The research is carried out with the intention of contributing to medical knowledge which can also be applied to populations outside of the direct research population."

The criterium for being subject to procedures or being required to follow rules of behaviour is typically more clear. The subject should be physically involved in the research to met this criterium. This means that retrospective research is not subject to the WMO.

In case a study falls within the scope of the WMO, the study dossier should be submitted to a local Medical Ethical Research Committee (MERC) for evaluation. In case there is doubt whether the study falls within the scope of the WMO, a local MERC can be contacted for their evaluation. In case they decide that it does fall within the scope of WMO, a full study dossier should be submitted to the local MERC. Carrying out a study which falls under the WMO without a positive decision from a local MERC is an illegal offence.

Study dossier to be submitted to MERC

The study dossier to be s consist of a large number of documents, including:

- Online registration of the study protocol
  This document provides a general overview of the study protocol and procedures and can be accessed online.
- The study protocol
  The study protocol gives an introduction on the research topic, the research objectives, study design, study population, treatment of subjects, investigational product, non-investigational

product, study methods, safety reporting, statistical analysis, ethical considerations, administrative aspects, monitoring and publication and a structured risk analysis.

- The investigational medical device dossier
  This dossier is required in case a non-CE-certified medical device is used, or a CE-certified medical device is used outside their intended use. The IMDD is based on Annex II of the Medical Device Directive (MDR). The IMDD should include technical documentation from the manufacturer to prove that the medical device adheres to the requirements of the MDR. The IMDD should provide enough information to ensure that an informed decision can be made with respect to the safety, performance and quality of the medical device used within the research.
- Patient information brochure and informed consent form
  In the patient information brochure, the participant is informed about the goal, rationale and procedures of the research. It also explains what is expected from the participant, what possible side effects may be and what the benefit of participation is. Finally it explains how patient data is stored and analysed, who has access to the data and what will happen with the data after the research has concluded.
  In the informed consent form, several statements are made. By signing the patient information brochure, the participant agrees with these statements. These include:
  - I have read the patient information brochure, had the chance to ask questions, these questions have been answered to satisfaction and I had enough time to consider participation?
  - I am aware that participation is voluntary and I am aware that I can stop participation without providing justification at any time.
  - I provide consent to the researchers to collect the personal data that are required to answer the research question.
  - I provide consent to the fact that other people that are mentioned in the patient information brochure to have access to the personal data.

  The informed consent form is signed by both the participant and the researcher. Both parties will receive a signed version of the informed consent form.
- If applicable, the questionnaires that will be used
- Insurance documents
- Resumes

All these documents will be reviewed and typically at least one of these documents needs revision before the MERC provides a positive advice with respect to the study dossier.

Process after approval

After the study is approved the MERC needs to be notified about the project start date before the study is actually started. In case a serious adverse event occurs, the MERC needs to be notified the moment the researcher became aware of serious adverse event. Examples of serious adverse events are death, severe disability and hospitalisation. Adverse events do not need to be submitted to the MERC directly as these are part of the yearly progress reports that need to be submitted.

4.5.3 General Data Protection Regulation (GDPR)

The GDPR (General Data Protection Regulation) is a European Union law that regulates the protection of personal data and the privacy of EU citizens. It came into force on May 25, 2018, and sets strict guidelines on how organizations must collect, store, process, and protect personal data.

Key aspects of the GDPR:

- **Clear and explicit consent:** Organizations must obtain explicit and clear consent from individuals to collect and process their personal data.

- **Right of access:** Individuals have the right to know what data is being collected about them, how it is used, and how long it will be retained.

- **Right to be forgotten**: Individuals can request that their personal data be deleted when it is no longer needed or if they withdraw their consent.

- **Data portability:** Users can request a copy of their personal data in a structured and transferable format.

- **Data protection by design and by default:** Organizations must implement security and privacy measures at all stages of data processing.

- **Data breach notification:** In the event of a data breach, organizations are required to notify the authorities and affected parties within 72 hours.

- **Severe fines:** Organizations that fail to comply with the GDPR can face significant fines, which can reach up to 4% of global annual revenue or €20 million, whichever is greater.

The main goal of the GDPR is to give citizens and residents control over their personal data and to simplify the regulatory environment for international business by unifying regulation within the EU.

Within the Dutch context, the GDPR is integrated into the WMO (see Section 3.5.2.). This means that when writing the research protocol as well as the patient information brochure. This, in turn, means that compliance to the GDPR is checked by the local accredited MERC. The Table below shows in which document the measures to adhere to these principles are described.

GDPR aspect	Described measures	Obtained consent
Clear and explicit consent	In the study protocol, the recruitment procedures are described as well as the way how informed consent is obtained in a general sense. These documents are not available to the study participant. The patient information brochure and informed consent form are specifically aimed at the study participant and their rights and obligations are clearly described. It also explicitly states what they are consenting to in case they participate in the study.	By signing the informed consent form.
Right of access	In the study protocol the type of data that is being collected is described as well as who has access, how it is stored and when it will be deleted. In the patient information brochure this information is also	By signing the informed consent form, the participant provides consent to the collection of the specified data, who has access, how it is stored and when it will be deleted.

	explained to the participant in layman's terms.	
Right to be forgotten	In the patient information brochure it is explained that participants can request that their data will be deleted.	By signing the informed consent form, the participant acknowledges that they are aware that they can request the data to be deleted.
Data portability	This is not a topic of the study protocol and/or patient information brochure. However, researcher will have to follow this aspect in case this is requested by the participant.	Not applicable.
Data protection by design and default	In the study protocol, the way the data are stored, where the data are stored and how the data are protected is described.	Not applicable.
Data breach notification	According to Dutch law, all entities are required to notify the Dutch Data Protection Authority within 72 hours after being notified about the data breach.	Not applicable.
Severe fines	Not adhering to the stipulations laid out in the WMO (see Section 3.5.2) will lead to severe fines. This includes not adhering to the GDPR as this is an integral part of the WMO.	Not applicable.

4.5.4 Declaration of Helsinki

The declaration of Helsinki is a statement that outlines the ethical principles to which medical research involving human subjects should adhere to. It is partly based on the declaration of Geneva. The declaration of Helsinki was first adopted by the 18th Assembly of the World Medical Association (WMA) in Helsinki in 1964 and has been amended several times. The latest amendment occurred during the 64th general assembly which was held in 2013 in Fortaleza, Brazil.

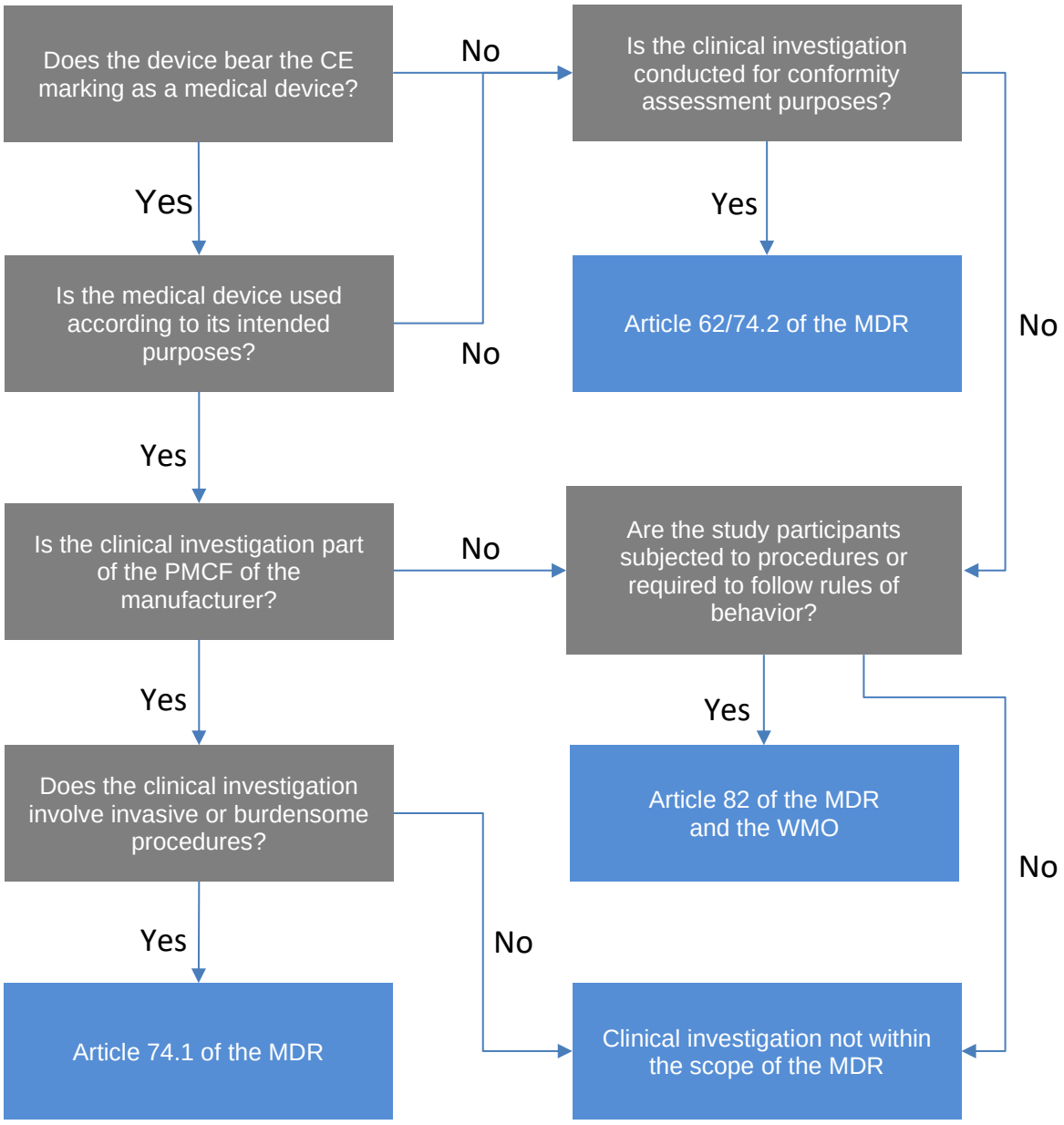
The declaration of Helsinki lists 10 specific topic areas. These includes:

1. Risks, burdens and benefits
2. Vulnerable groups and individuals
3. Scientific requirements and research protocols
4. Research ethics committees
5. Privacy and confidentiality
6. Informed consent
7. Use of placebo
8. Post-trial provisions
9. Research registration and publication and dissemination of results
10. Unproven interventions in clinical practice

The declaration of Helsinki is integrated in the WMO which means that these topic areas are taken into consideration when the local accredited MERC is reviewing the study protocol.

4.5.5 Medical device regulation

The medical device regulation (MDR) has been enforced since 26 May 2021 and replaced the medical device directive and the active implantable medical device directive. The goal of the MDR is to improve patient safety as well as ensure that innovative medical devices will remain available to patients. Three different articles of the MDR may be applicable for performing research with medical devices. These are article 62, 74 and 82. With the following scheme a researcher can determine if and, if so, which articles of the MDR apply.



4.5.6 ISO 14155: Clinical investigation of medical devices for human subjects – Good clinical practice

This standard addresses good clinical practice (GCP) procedures for the design, conduct, recording and reporting of clinical investigations carried out in human subjects to assess the clinical performance of effectiveness and safety of medical devices. This document specifies general requirements intended to protect the rights, safety and well-being of human subjects, ensure the scientific conduct of the clinical investigation and the credibility of the clinical investigation results, define the responsibilities of the sponsor and principal investigator and assist sponsors, investigators, ethics committees, regulatory authorities and other bodies involved in the conformity assessment of medical devices.

To be able to execute research that falls under the scope of the WMO (see Section 3.5.2) it is mandatory that the (primary) researchers and all those involved in the execution of the research has followed a GCP training. MERC do not provide a positive advice for study protocols that have been submitted by a (primary) researcher that has not followed a GCP training.

This means that research that falls within the scope of the WMO (see Section 3.5.2), the procedures laid out in ISO 14155 will be followed. For research that does not fall within the scope of the WMO, this is not mandatory.

4.5.7 Application of regulations within TREAT

For the Dutch use case, either an exemption of the WMO (see Section 3.5.2) will be asked or a full study protocol will be submitted for evaluation. In case a study is exempt from the WMO, the GDPR and the Declaration of Helsinki will still apply and, therefore, will be followed. In case a full study protocol will be submitted to the local accredited MERC, all regulations specified in Section 3.5 apply (with the potential exception of the MDR) and adherence will be checked before a positive advice is given.

5. Plan for obtaining Informed Consent from Participants

5.1 Methods for clearly explaining project objectives to participants.

A notice will be developed for the project that will inform participants of project objectives and how the TREAT project will collect, use, disclose and safeguard their personal data. The notice must be made readily accessible prior to personal data collection, and easy to understand, allowing data subjects to make an informed decision when providing consent for the processing of their personal data.

The notice shall include:

- The types/ categories of personal data collected and the means by which personal data is collected.
- The purpose for collecting personal data, including any intended uses and/or disclosures.
- The general categories of whom may have access to the personal data, including sub processors.
- The data subject's right to have access to the information and to have it rectified.
- If personal data will be de-identified, aggregated or anonymized and if de-identified/anonymous information will be disclosed outside the project.
- The use of any automated decision-making or processing.
- The right to opt-out of any processing not directly aligned with the project's objectives, including the right to withdraw consent of personal data processing and any consequences of withdrawal.
- A general description of safeguards.
- The location(s) where personal data will be kept.
- The period of time or criteria for retention of personal data.
- Contact information for someone who can answer individual questions, and the right to lodge a complaint.

In addition to providing notice to data subjects, individuals working directly with data subjects should be given a copy of the notice for review. They should familiarize themselves with the notice, that they can verbally assist data subjects in understanding the project's collection, use, retention and disclosure.

5.2 Steps for ensuring that informed consent is voluntary and non-coercive.

To ensure consent is voluntary, the project will take the following safeguards:

- Notice, in the form of a written privacy notice will be provided prior to collection, to confirm data subjects can make informed decisions prior to participating.
- Consent for any processing that is not mandatory for the project to operate must be opt-in. For example: consent to disclose personal data to optional third-parties, consent to communicate with the data subject beyond regulatory and participatory requirements, consent to use personal data for optional processing that may of interest.
- Data subjects will be reminded in the notice of their right to withdraw consent at any time, and the implications of withdrawal. Withdrawal of consent will not be retroactive or apply to data that has been previously de-identified/ anonymized.
- Through policy or code of conduct the project will communicate to internal participants/ staff/ contractors that they may not impose penalties over individuals choosing to exercise their right to withhold or withdraw consent.

5.3 Mechanisms for ensuring confidentiality and the right of participants to withdraw consent at any time.

To ensure the right of participants to withdraw consent at any time, the project must have:

- Information on the right to withdraw, provided prior to information collection.
- A process in place for handling requests to withdraw, including verification of the request and providing information on the consequences of withdrawal.
- Optional consent for additional purposes of processing.
- The ability for any technical systems to stop or limit the processing of personal data upon individual request. This can include:
    - The ability to deactivate personal data from electronic processing.
    - The ability to delete/ erase personal data to prevent further processing.
    - The ability to limit who has access to personal data for processing.

Further to the right to withdraw consent, participants who choose to permit their personal data to be used as part of TREAT must have confidence their data will remain confidential. The TREAT project will protect the confidentiality of personal data through:

- Use of confidentiality agreements, signed by internal participants of TREAT, including contractors, with access to or who will be operating near personal data.
- A code of conduct, signed off by all internal participants and contractors.
- Training for internal participants on privacy and security best practices, the GDPR and PIPEDA.
- Administrative policies that include protection of privacy, security programs, and documentation of safeguards.
- Technical and physical safeguards to prevent theft, loss, unauthorized access, use, processing or disclosure of personal data.
- Review of all sub-processor privacy and security practices, to confirm sub-processors retaining and/or processing personal data meet TREAT privacy and security requirements.
- Contracts with sub-processors to confirm limited use of personal data only for the purpose of suppling services. Contract should include requirements on general safeguards, compliance with applicable privacy legislations, contact in the event of an incident, and what happens to TREAT data if the services are terminated.

6. Plan for the management of Sensitive Data and Privacy Protection

6.1 Strategies for storing processing and anonymizing participants' personal data.

Where personal data for the TREAT project will be retained in a digital environment, cloud storage is ideal. Use of a Cloud provider, particularly one who abides by the Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) program, implements a robust set of physical and technical security requirements that can be further improved upon by TREAT project policies and security standards. Special attention will be needed to confirm that TREAT project data is retained at limited facilities deliberately selected by the project to meet the GDPR's data residency restrictions.

Anonymization of personal data involves the permanent removal of identifying information in a way that no longer allows the individual to be identified, safeguarding individual privacy. For anonymization of personal data, consultation with a subject matter expert is advised, esp. as the TREAT project will be using artificial intelligence for personal data processing, which can increase the risk of re-identification unless a strong method of anonymization is used. Examples of sophisticated anonymization techniques include k-Anonymity, I-Diversity, t-Closeness and Differential Privacy and Federated Learning. When choosing a methodology, a preliminary analysis of the risk of re-identification is advised.

Whatever anonymization methodology the TREAT project chooses to employ should be documented. This in particular is a requirement if the TREAT project must comply with Quebec's ARPPIPS.

Documentation should include:

- A description of the personal data to be anonymized.
- The purpose of anonymization.
- That the process of anonymization will be carried out by an individual qualified in the field.
- The anonymization techniques used.
- Protection and security measures to protect against re-identification.
- Once information is processed, an analysis of re-identification risk should be done, with the report including a summary of the results.
- Date the analysis of re-identification risk was conducted.

6.2 Policies to limit access to sensitive data to authorized personnel only.

To ensure limited access to sensitive data, the project will take the following safeguards:

- Policies on Access Management and Control.
    - Access will be granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner. The TREAT project will determine if context-based access (access control based on the context of a transaction), role-based access (user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role) or user-based access (a security mechanism used to gran users of a system access based on the identity of the user) will be implemented.
    - Access will be revoked upon termination of the user from the project, or upon changes to the user's responsibilities where access to sensitive data is no longer required.

- Policies on Authentication.
    - Unique user identification (user id) and authentication is required for all systems that maintain or access Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.
    - If authentication relies on the combination of user id and password, password requirements will be documented. Password requirements may include, but are not limited to minimum alphanumeric characters, time-out, user reminders on password sharing restrictions and practices when selecting passwords to avoid.
    - Passwords must always be encrypted in transit and may never be retained in plaintext.
    - Default vendor passwords must always be changed immediately following the installation of systems or software.
    - Multi-Factor Authentication (MFA) is encouraged for access of sensitive data.
- Audits.
    - Access will be reviewed / audited on regular intervals to confirm policy compliance is in place.

6.3 Technical measures to protect data against security breaches (encryption, access control, etc.).

Security Features for the TREAT project should include:

- Access Controls: access to confidential information on a need-to-know basis.
- Authentication: username and password authentication for end-users. Multifactor authentication should be in place for access to sensitive data or environments.
- Backups
- Change Management
- Code Review and Software Policy
- Controls against malware
- Encryption in transit and at rest
- Event Logging
- Firewalls and Network Controls
- Password Management
- Patch Management
- Physical security
- Testing
- Threat/ Risk Assessments, and third-party attestation
- Vendor Management

6.4 Plans to comply with data deletion after a certain period or at the end of the study.

Under privacy laws, when personal data is no longer needed for the purpose by which it was collected, and if there is no legal / regulatory reason for retention, data must be destroyed. This will involve:

- At the end of the retention period, personal data and any copies of the personal data that are no longer required for the purposes for which it was collected, will be destroyed or rendered anonymous.

- If physical records such as paper documents are part of the project, they should be shredded when no longer needed or required to be maintained.

- Electronic documents and other digitally maintained data should be permanently deleted when no longer needed. When destroying electronic data ensure that the proper method is used so that the data cannot be recovered (see Table).

- Digital storage media (electronic devices including desktops computers and portable devices) should be degassed and/or destroyed when no longer needed. External media (CD. DVD, diskettes, USB drives) must never be thrown in the regular office trash. They should be destroyed by shredding. Identifying logos or markings should be removed.

- Where personal data is rendered anonymous, an effective anonymization or pseudonymization algorithm and program will be applied; this will include anonymization with applicable regulations. After anonymization or pseudonymization the source files will be destroyed in a secure manner.

- If third-party sub-processors are in use to destroy personal data, operations must include secure transport of the information to the destruction facility, and providing the TREAT project with a record of destruction once all personal data is destroyed.

- When equipment that includes media or devices containing personal data, application software or security critical system data is sent out for repair, reuse or disposal (e.g. hard drives, flash drives) the media or devices containing personal data will be removed, destroyed or permanently erased.

- Subcontractors provide that, upon termination of the contract, they will return or destroy/dispose of all patient health information. In cases where the return or destruction/disposal is not feasible, the contract limits the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.

Destruction Method	Media	Considerations
Secure Erasure: includes using special software to securely erase data or encrypted volume without causing physical damage to the device	• Solid State Drives (SSD) • HDD Hard Drives (internal or external)	• Use of certified software or third-party suppliers recommended.
Shredding: involves cutting of print media.	• Print media • Optical Disks	• Should always be conducted in a secure location. • Use of cross-cutting shredding techniques for sensitive information recommended.
Degaussing: exposing magnetic media to strong magnetic fields. Eliminates stored information but renders media type unusable.	• HDD Hard Drives • Some types of magnetic media	• Should always be conducted in a secure location.
Overwriting: destroys sensitive data by recording non-sensitive information or zeros over past storage. I	• HDD Hard drives • Mobile devices	• Repeat 2-3 times for drive media. • Use internal software, including factory resets, on mobile devices. • Ineffective for optical disks.
Physical destruction: includes physical methods not identified	• Print media	• Should always be conducted in a secure location.

above, such as incineration, pulverization or melting of storage media.	• SDD and HDD Drives • Mobile Devices • Electronic Drives • Optical disks (CD, DVD)	• The use of physical destruction in addition to degaussing or overwriting is considered the most secure method for destroying media.

7. Conclusions

The legal and ethical analysis carried out in this report establishes a solid foundation for ensuring regulatory compliance in data handling within the TREAT project. The following conclusions and recommendations are key for the next phases of the project:

Regulatory compliance: It is essential to implement technical measures such as encryption and anonymization to ensure compliance with regulations such as the GDPR and the LOPDGDD.

Informed consent: Priority should be given to creating clear and accessible interfaces for obtaining consent from participants, ensuring that they can revoke it at any time.

Risk management: Data impact assessments (DPIA) should be carried out periodically to identify and mitigate new risks associated with handling sensitive data.

Staff training: Train all those involved in privacy and security best practices, ensuring adherence to local and international regulations.

These measures not only ensure legal compliance but also reinforce the trust of participants in the project.

8. References

- Reglamento General de Protección de Datos (GDPR). European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. Recuperado de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
- Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD). Agencia Española de Protección de Datos (AEPD). (2018). BOE-A-2018-16673. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673
- ISO 27001: Seguridad de la Información. International Organization for Standardization. (2021). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection. Recuperado de https://www.iso.org/standard/82875.html
- Consejo Internacional de Investigaciones Médicas (CIOMS). Council for International Organizations of Medical Sciences (CIOMS). (2016). International Ethical Guidelines for Health-Related Research Involving Humans. Recuperado de https://cioms.ch/publications/product/international-ethical-guidelines-for-health-related-research-involving-humans/
- Cloud Security Alliance. (2021). Security, Trust, Assurance, and Risk (STAR) Program. Recuperado de https://cloudsecurityalliance.org/star/
- Reglamento General de Protección de Datos (GDPR). European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. Recuperado de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
- Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD). Agencia Española de Protección de Datos (AEPD). (2018). BOE-A-2018-16673. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673
- ISO 27001: Seguridad de la Información. International Organization for Standardization. (2021). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection. Recuperado de https://www.iso.org/standard/82875.html
- Consejo Internacional de Investigaciones Médicas (CIOMS). Council for International Organizations of Medical Sciences (CIOMS). (2016). International Ethical Guidelines for Health-Related Research Involving Humans. Recuperado de https://cioms.ch/publications/product/international-ethical-guidelines-for-health-related-research-involving-humans/
- Cloud Security Alliance. (2021). Security, Trust, Assurance, and Risk (STAR) Program. Recuperado de https://cloudsecurityalliance.org/star/
- Health Insurance Portability and Accountability Act (HIPAA). U.S. Department of Health & Human Services. (1996). Recuperado de https://www.hhs.gov/hipaa/index.html
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). Government of Canada. (2000). Recuperado de https://laws-lois.justice.gc.ca/eng/acts/P-8.6/
- Fair Information Practice Principles (FIPPs). Federal Trade Commission. (2000). Recuperado de https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report
- European Commission. (2021). Ethics guidelines for trustworthy AI. Recuperado de https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
- HL7 International. (2020). Fast Healthcare Interoperability Resources (FHIR). Recuperado de https://www.hl7.org/fhir/

- International Organization for Standardization. (2021). ISO 22301:2019 - Business continuity management systems. Recuperado de https://www.iso.org/standard/75106.html
- European Data Protection Board (EDPB). (2020). Guidelines on Data Protection Impact Assessment (DPIA). Recuperado de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dpia_final_en.pdf
- National Institute of Standards and Technology (NIST). (2020). Cybersecurity Framework. Recuperado de https://www.nist.gov/cyberframework
- World Health Organization (WHO). (2021). Guidance on Artificial Intelligence in Health. Recuperado de https://www.who.int/publications/i/item/9789240029200
- European Medicines Agency (EMA). (2020). Data protection in clinical trials. Recuperado de https://www.ema.europa.eu/en/human-regulatory/research-development/data-protection