ITEA 4

PRocedure Optimization and data-driven eFficiency Improvement in healthcare environmenTs

DELIVERABLE D1.3

Legal and ethical requirements

Project number:	ITEA 22021
Document version:	v1.0
Edited by:	Paula Savolainen, Kaisa Jokela
Date:	28.11.2025

HISTORY

Document version #	Date	Remarks
V0.1	4.4.2025	The initial version of the document
V0.2	19.6.2025	The working version for the summer period
V0.3	5.11.2025	Document ready for the review
V0.4	18.11.2025	Document with comments from the reviewers
V0.5	26.11.2025	Modified version after the review
V1.0	28.11.2025	Final version

Deliverable review procedure:

- **2 weeks before due date**: deliverable owner sends deliverable –approved by WP leader– to Project Manager.
- **Upfront** PM assigns a co-reviewer from the PMT group to cross check the deliverable.
- **1 week before due date**: co-reviewer provides input to deliverable owner.
- **Due date:** deliverable owner sends the final version of the deliverable to PM and co-reviewer.

Table of Contents

Acronyms

Acronym	Description
CE	Conformité Européenne (European Conformity marking)
CNPD	Comissão Nacional de Proteção de Dados (Portuguese Data Protection Authority)
CRA	Cyber Resilience Act
DGA	Data Governance Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Digital Services Act
EC	Ethics Committee
ECTS	European Credit Transfer and Accumulation System
EHDS	European Health Data Space
EHR	Electronic Health Record
ENISA	European Union Agency for Cybersecurity
EU AI ACT	European Union Artificial Intelligence Act
EUDAMED	European Database on Medical Devices
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation
HDAB	Health Data Access Body
HL7	Health Level Seven (interoperability standard)
ICN	International Council of Nurses
IEC	International Electrotechnical Commission
IRB	Institutional Review Board
ISO	International Organization for Standardization
IVDR	In Vitro Diagnostic Medical Devices Regulation
KELA	The Social Insurance Institution of Finland
KPI	Key Performance Indicators
LOVe	Safe Pharmacotherapy (Finnish: Lääkehoidon osaamisen varmistaminen)
MDR	Medical Device Regulation
MDSW	Medical Device Software
NCSC-FI	National Cyber Security Centre Finland
NHS	National Health Service
NIS2	Network and Information Security Directive 2
OR	Operating Room
PCCP	Predetermined Change Control Plans
QA	Quality Assurance
REC	Research Ethics Committee
SaMD	Software as a Medical Device
SNOMED CT	Systematized Nomenclature of Medicine – Clinical Terms
UC	Use Case
WP	Work Package

1 Introduction

PROFIT (Procedure Optimization and data-driven Operational eFficiency In healthcare environmenTs) is a Europe-wide R&D project that brings together hospitals, technology providers and research organisations to streamline clinical workflows with trusted Artificial Intelligence (AI) and data solutions. Across six complementary use cases, smart alarm response, clinical-grade AI deployment, real-time asset tracking and sterilisation, digital home care, AI-assisted clinical documentation and patient-pathway orchestration, PROFIT develops:

- a vendor-neutral, medical-grade compute platform and continuous QA framework for safe, interoperable AI in care settings;
- privacy-preserving data-management tools that comply with GDPR, the EU AI Act and MDR; and
- context-aware decision-support applications that improve patient outcomes, staff experience and operational efficiency while reducing costs.

The ultimate aim is to help European healthcare systems deliver faster, safer and more personalised care through responsible, legally compliant innovation.

In a project like PROFIT, which develops and deploys AI solutions across hospitals, home care, clinical documentation, patient pathways and other areas, ethical and legislative considerations are essential from the outset. Healthcare AI systems handle highly sensitive patient information and can directly influence clinical decisions, so mistakes or misuse can have serious consequences. As noted in recent literature, the growing integration of AI into care requires effective governance to address regulatory, ethical and trust-related concerns, ensuring appropriateness, effectiveness, patient safety, accountability and clinician confidence in AI tools. In the EU's policy view, robust frameworks are needed to mitigate AI's risks while enabling ethical, secure and practical implementation in healthcare. In short, ethics and regulatory compliance are fundamental to the safe and successful development of healthcare AI.

Sensitive health data is a core concern. AI-driven healthcare solutions rely on personal health data (e.g. medical records), which EU law classifies as highly sensitive. Under the General Data Protection Regulation (GDPR), health data receives special protection due to its sensitivity and the potential for abuse. A data leak or misuse of medical records can be devastating, undermining patient privacy and dignity and enabling discrimination. Strict data protection measures and privacy-by-design solutions are therefore paramount. Patients and providers must be confident that an AI system will guard personal data and use it responsibly. Ethical data management, including informed consent, secure handling of data, transparency in data use and robust cybersecurity, is required to ensure individuals' rights and expectations of privacy. In the PROFIT project, treating patient data ethically and lawfully fosters trust, which is essential for the sustainable deployment of AI solutions in healthcare.

The PROFIT project involves six innovative healthcare use cases, ranging from smart alarm management to AI-assisted clinical documentation and care pathway orchestration. Each use case must be evaluated through the lens of legal and ethical requirements to ensure compliance with European regulations and adherence to high ethical standards. This document provides a comprehensive assessment of the relevant frameworks – including the General Data Protection Regulation (GDPR), the proposed EU Artificial Intelligence Act, the EU Medical Device Regulation (MDR) and the European Commission's Ethics Guidelines for Trustworthy AI – as well as bioethical principles like those in the Declaration of Helsinki. We map specific ethical challenges in each use case to these frameworks and discuss how

PROFIT's approach aligns with or mitigates the challenges. The goal is to ensure that all PROFIT innovations respect principles of fairness, transparency (and explainability), accountability and other core values, while complying with legal obligations.

The PROFIT project's six use cases, while diverse in application, share common ethical and legal imperatives. By proactively mapping these use cases against major European frameworks, GDPR ensuring data privacy, the EU AI Act imposing rigorous standards for high-risk AI, MDR guaranteeing medical device safety and the Ethics Guidelines for Trustworthy AI emphasising principles like transparency, fairness and accountability, we ensure that innovation does not outpace responsibility. In each scenario, specific challenges have been identified (from alarm safety to documentation accuracy to equitable care access) and PROFIT's approach includes concrete measures to align with or mitigate those challenges: privacy-aware technologies, continuous AI performance monitoring, stakeholder engagement and compliance-by-design for regulations.

Ultimately, this legal and ethical requirements document underlines that patient welfare, data protection and trust are at the core of PROFIT's healthcare innovations. By adhering to European legal mandates and ethical standards, PROFIT meets its obligations and builds a foundation of trust with users (patients and professionals alike). This trust is crucial for the successful adoption of AI in healthcare. The comparative analysis per use case demonstrates that while the contexts differ (acute care, home care, operational efficiency), the commitment to fairness, transparency/explainability, accountability and safety remains constant. PROFIT's alignment with frameworks like the Declaration of Helsinki (putting patient welfare first) and the EU's trustworthy AI requirements shows a comprehensive approach: from respecting individual rights and agency to ensuring societal benefit through improved healthcare outcomes.

This document limits its legislative review to EU-level considerations, in alignment with PROFIT's scope as an EU-wide project operating exclusively within European jurisdictions. As PROFIT moves from design to implementation, ongoing ethical assessment and legal compliance checks will be vital. This will include updating Data Protection Impact Assessments, obtaining necessary regulatory approvals for AI components and involving ethics committees where human-centric trials are conducted. By doing so, the PROFIT consortium can confidently demonstrate that its solutions are not only innovative and effective, but also lawful, ethically sound and worth of the public's trust.

A large group of users of the technology being developed in PROFIT project is nurses. Therefore, the document includes an exemplary description of the ethical principles of nursing, the laws regulating nursing, and how these are taken into account during nursing education.

This document was produced by a working group consisting of use case leaders, researchers, and data protection and legal experts. Data protection, legal and ethical experts created the structure, some of the content, and reviewed the final document. However, it should be noted that the use case leaders were responsible for producing especially use case-specific content. This working method created the conditions for a broader internal processing of the topic in the companies participating in the project and thus facilitated the companies' communal learning. The creation of the content was therefore not outsourced to data protection, legal or ethical experts, but rather the technology experts have devoted themselves in-depth to considering data processing and its dimensions when producing the content of the document. The chosen working method is reflected in the content of the document, as the contents of the subchapters have not been strictly harmonized. This

makes it easier to use the document as a support document for the developers of use case technologies.

2 Ethical viewpoints

The European Commission's Ethics Guidelines for Trustworthy AI

The European Commission's Ethics Guidelines for Trustworthy AI provide a framework of ethical principles that AI systems should meet. PROFIT's use cases are evaluated against these seven key requirements, which include:

- **Human Agency and Oversight**: AI should augment and complement, not replace, human decision-making, increasing the importance of implementing human oversight mechanisms like human-in-the-loop or human override. In healthcare, this means clinicians and patients must be granted the right to control, supervise, verify, or override critical points in the workflow. PROFIT's systems are designed to empower professionals and support decision making while still allowing and advocating for human judgment in critical decisions. Each use case considers individually how human oversight is applied and exercised.
- **Technical Robustness and Safety**: AI must be reliable and secure, complemented with strategies to minimize and prevent risk of harm. This requirement aligns with MDR's objective to ensure safe and effective medical devices, as well as the bioethical principle of non-maleficence. Further, it is complemented with the UNESCO Recommendation on the Ethics of AI, stating the importance of continuous monitoring, validation and testing of the safety, accuracy and robustness of the developed systems throughout their entire technology life cycle. PROFIT addresses this by ensuring fallback plans and accuracy testing for all AI components. The project's emphasis on performance monitoring and validation studies exemplifies technical robustness in practice. It also includes considering cybersecurity measures and planning of secure communication protocols such as implementing Ascon cryptographic algorithms, as attacks or failures in healthcare AI security could endanger patients through data manipulation or misuse.
- **Privacy and Data Governance**: Echoing GDPR requirements for processing personal data, the guidelines stress privacy, data quality and proper data handling. PROFIT's privacy-by-design approach, including but not limited to encryption, access control and federated learning model training without sharing raw data, ensures that personal health data are used ethically and securely. Data governance also means ensuring data integrity and avoiding misuse, such as ensuring that any additional data collected during the project is not repurposed in a way that violates the informed consent of the participating patients or clinicians.
- **Transparency (and Explainability)**: AI systems and their decisions should be transparent and explainable to the extent possible. Relevant stakeholders, including clinicians, patients and administrators, should understand when AI is being used and how it influences outcomes. The guidelines specifically note that "AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned" and humans "need to be aware that they are interacting with an AI system and must be informed of the system's capabilities and limitations". In PROFIT, transparency is addressed in multiple ways, for example by developing user interfaces that clearly indicate AI-driven suggestions or analyses. PROFIT's AI solutions aim to provide rationale where feasible, for example by indicating the data patterns or guidelines leading to the suggestions or recommendations provided by the system, increasing end-user trust towards the system.
- **Diversity, Non-Discrimination and Fairness**: AI should avoid unfair bias and be accessible to all users. In healthcare, this translates to ensuring that AI does not inadvertently discriminate against any population group, including older adults, minorities. PROFIT must ensure that training data for AI algorithms are

representative of the patient populations to prevent biased outcomes. This includes, for example, assuring that the prioritization of patients is not based on irrelevant factors but on their clinical needs, or that speech recognition systems accurately understand different accents or dialects to serve all clinicians and patients fairly. The involvement of stakeholders in design is also emphasized as part of fairness: PROFIT indeed engages end-users in co-development and feedback loops to capture diverse perspectives and needs. This co-creation helps identify potential biases or usability issues early, fostering inclusivity. Additionally, some use cases directly promote fairness in access to care, for example by extending services to those who might have difficulty reaching clinics, improving equity in healthcare delivery. Ensuring accessibility of these digital tools, such as user-friendly design for those with low digital literacy or disabilities, is an important ethical requirement the project considers.

- **Societal and Environmental Well-being**: AI should benefit society and the environment. PROFIT's overarching goal aligns with societal well-being: better patient outcomes, improved patient and clinician experience, and lower cost of care. By optimizing hospital workflows and home care, the project seeks to reduce burdens on healthcare systems by freeing resources for more patient-facing care, as well as improve quality of life for patients. While environmental impacts are not a primary focus, efficient processes and digital solutions may decrease the amount of healthcare generated waste and increase resource efficiency, as well as reduce unnecessary travel as fewer hospital readmissions or visits due to better home monitoring could lower transportation emissions. All these contribute to a more sustainable and patient-centered healthcare model, aligning with this key requirement.
- **Accountability**: Mechanisms to assign responsibility for AI actions and outcomes are integral. In PROFIT's context, accountability is critical because decisions supported by the AI systems have an impact on human health, well-being and safety. Legally, this ties into liability – for instance, the end-user organisations and system manufacturers need clear processes to investigate and address potential system malfunctions or failures. Accountability entails all use of data, the AI, and the produced outcomes, for example by respecting intellectual property rights, including copyrights and open-source data licenses. Ethically, PROFIT ensures accountability by keeping humans in the loop and maintaining audit logs of AI decisions. Auditability is explicitly mentioned in the guidelines as key to accountability. PROFIT's systems are being developed to log AI recommendations and actions, so they can be reviewed and audited by quality committees or regulators if needed. Moreover, clarity about who is responsible for final decisions is maintained: for example, the clinician remains responsible for a diagnosis even if assisted by an AI tool, and the project's training for end users will reinforce that AI is a support tool, not an infallible oracle. PROFIT also envisions providing redress mechanisms – if an AI causes an error or a patient experiences an issue, there should be a way to rectify and learn from it. By integrating continuous improvement and oversight, the project embodies the principle that someone (developers, providers, or users) is answerable for the AI's behavior.

In summary, the Trustworthy AI principles map closely to both the legal requirements and the biomedical ethics tenets, such as human agency and autonomy, fairness and justice, non-maleficence and safety. PROFIT's commitment to these principles is embedded in its design choices and objectives, which we will detail per use case in Chapter 4.

Adherence to the Declaration of Helsinki and Medical Ethics

Healthcare innovations must also adhere to broader bioethical standards that protect patient rights and welfare. The World Medical Association's Declaration of Helsinki (2013) is a cornerstone for any research or clinical investigation involving humans. It mandates that “the participant’s welfare must always take precedence over the interests of science and society”. This is highly relevant for PROFIT: while the project pursues technological advancement and efficiency, it must never compromise patient care quality or safety in the process. Any pilot deployments of PROFIT solutions in clinical settings should undergo ethics committee (EC) approval and informed consent from participants, in line with Helsinki principles. For example, if patients are involved in testing the digital home care platform or AI documentation tool, they have a right to be informed about what data is collected and to consent to any experimental aspects. The Declaration also highlights risk-benefit assessment and independent review – PROFIT’s use cases have undergone analysis of potential risks (e.g. risk of alarm misrouting, risk of privacy breaches) versus benefits and the project includes stakeholders and ethical experts to review these considerations.

Other foundational bioethics principles from frameworks like Beauchamp and Childress’s “Four Principles” (autonomy, beneficence, non-maleficence, justice) further guide the evaluation:

- **Autonomy**: Respecting patients’ and clinicians’ autonomy reflects the values of personal freedom and choice. For instance, patients should retain choice in accepting or declining digital home monitoring or AI-driven advice. For clinicians, systems should be developed to support their professional judgment consistent with their professional ethical code of conduct, not to override it. In PROFIT, participant autonomy is accounted for throughout the entire technology lifecycle through informed consent based on three principles: disclosure of relevant information, capacity to make an informed decision, and voluntariness and the right to withdraw consent at any time.
- **Beneficence**: A shared objective of PROFIT use cases is to demonstrably benefit patients – for example faster response to alarms improves outcomes, better documentation can enhance care continuity, orchestrated pathways can reduce suffering from delays. Each use case is designed with a clear benefit in mind, addressing current healthcare weaknesses (as identified in deliverable D1.1) to improve quality of care.
- **Non-Maleficence**: Avoiding harm is imperative. PROFIT must ensure that new risks introduced by technology are minimised through continous testing, validation and safeguards. For example, algorithms are rigorously tested so they do not introduce dangerous errors and backup procedures exist if an AI system fails (e.g. a manual alarm escalation protocol remains available).
- **Justice**: Equity in healthcare delivery – ensuring fair access and not exacerbating disparities. PROFIT’s focus on home care access, as well as careful attention that AI models treat all patients fairly, supports distributive justice. Additionally, fairness toward healthcare staff (like equitable workload distribution in alarm response) is considered, improving the work environment ethically.

In Europe, the EU Charter of Fundamental Rights and instruments like the Oviedo Convention on human rights in biomedicine also inform legal-ethical compliance – they underscore rights to privacy, integrity and equitable access to healthcare. While not explicitly mentioned in project documents, these values are implicit in the regulations

Research-Ethics Governance Process

Innovation in sensitive domains, such as AI-enabled healthcare, demands a rigorous, multi-layered ethics process that is embedded from proposal through post-deployment. For PROFIT, the ethics pathway begins with an EU ethics self-assessment at the proposal stage. This internal exercise requires partners to identify any use of special-category data, involvement of vulnerable participants, deployment of high-risk AI or dual-use technologies, and to outline proportional safeguards. The self-assessment forms the basis for external review and demonstrates that the consortium has recognised its ethical responsibilities from the outset.

Given the scale and sensitivity of the data flows in PROFIT, a Data-Protection Impact Assessment (DPIA) is mandatory under GDPR Article 35. The DPIA maps data lifecycles for each use case, pinpoints risks such as re-identification, accidental disclosure, or function creep, and specifies technical and organisational controls, including encryption in transit and at rest, strict role-based access, pseudonymisation, secure cloud configurations, and breach-notification workflows.

The full study protocol, participant information leaflets, consent forms, study materials, a detailed Data Management Plan, and the DPIA, are submitted to an EC in every country where human data will be collected. ECs, such as Research Ethics Committees (REC) and Institutional Review Boards (IRB), are designated institution-based or independent committees entrusted to review and oversee biomedical research involving human participants. The primary role of the ECs is to assure that proper measures are undertaken to protect the welfare, safety and rights of the research participants, with special emphasis on safeguarding the most vulnerable populations. The review is necessary for all research that poses more than minimal risk to the participants, such as deviations from informed consent or intervening with the physical integrity of the research participants, but it also can be provided following a request from funding organizations, research collaborators or publishers.

ECs evaluate the study for its scientific validity, the risk–benefit balance, protection of vulnerable groups, informed-consent procedures, and alignment with the ethical principles set in Declaration of Helsinki. The ECs hold the right to approve, modify, reject, or recommend revisions or clarifications to the study protocol and its attachments. No recruitment or data collection may start until a written approval letter has been secured, and an ECs approval process cannot be initiated once the research has begun. In cases where the study protocol of an EC approved study needs to be modified, for example, due to changes in participant recruitment or data collection, the approval needs to be re-reviewed. Following the ECs approval, the necessary research permits are sought from the organisations in which the data collection will take place. The research permit processes vary between the countries and organisations, but typically the required documents attached to the research permit application are in line with the document requirements set by the ECs, complemented with an EC approval letter and possible data access requirements or resource needs.

Where software components qualify simultaneously as Medical Device Software (MDSW) and high-risk AI systems under the EU AI Act, dual regulatory submissions are required. The clinical-investigation plan, risk-management file and post-market surveillance plan are submitted to a notified body and the national competent authority in parallel with EC review. Approval from all three bodies, the EC, the notified body and the competent authority must be obtained before patient-facing pilots begin.

Ethical governance is a continuous process rather than a one-off event. Serious adverse events, data-protection incidents, or unanticipated findings trigger immediate reporting to the EC, the Data Protection Officer and relevant regulators. Annual progress reports keep oversight bodies informed about recruitment numbers, emerging risks and any protocol amendments.

PROFIT adopts the European Commission's Ethics Guidelines for Trustworthy AI by involving clinicians, patients, and carers in co-design workshops, clearly labelling AI-generated outputs, and providing channels for user feedback and redress. Before dissemination, all datasets and models undergo a re-identification of risk assessment. Only data necessary for legitimate scientific aims is shared and only under controlled-access agreements that adhere to principles on participant consent.

3 Legislation

Although legislation changes slowly, it does change. And examining the legislation related to the content of a project is like jumping on a moving train - and then jumping off it halfway through. Six months after the completion of this document, some parts will be already outdated, and some new laws should be considered. The working group was aware of this and kept in mind that the content of the document must be useful to the project partners rather than to the public audience.

The working group limited its legislative review to EU-level considerations, in alignment with PROFIT's scope as an EU-wide project operating exclusively within European jurisdictions. Moreover, this chapter discusses legislative stipulations/directives that are relevant in the context of PROFIT use cases. National laws - if necessary - are examined on a use case-by-use case basis.

3.1 Data Governance Act (DGA)

The Data Governance Act creates a legal framework to enable secure and trustworthy data sharing across the EU, particularly in the following areas:

- Public sector data reuse, especially for non-commercial innovation,
- Data altruism, where individuals or entities voluntarily share data for the common good (e.g. research, healthcare),
- Data intermediation services, which act as neutral brokers between data holders and users.

DGA does not impose direct obligations on medical device or software manufacturers, but it may become relevant if the system: uses or contributes to shared health data spaces (e.g. European Health Data Space (EHDS) or national health data platforms, DGA sets out rules for fair and secure data sharing); involves secondary use of public sector or research data; engages in data altruism (e.g. if the solution enables voluntary data donation by patients, for example to improve AI models, it will fall under the DGA's data altruism framework).

DGA provides a legal framework that enables, but does not mandate, data sharing, while promoting trust and safeguards through neutral governance, data protection and alignment with GDPR and sector-specific regulations (such as the Medical Device Regulation). It is particularly supportive of innovation in areas like AI, medical research and public interest services, by facilitating broader and safer access to high-value datasets.

The DGA entered into force on 23 June 2022. It became applicable across the EU starting 24 September 2023, and organizations are expected to comply from that date onward.

Further information on the Data Governance Act (DGA) can be found at the following source: European Data Governance Act | Shaping Europe's digital future.

3.2 European Health Data Space (EHDS)

The European Health Data Space (EHDS) Regulation establishes a unified legal and technical framework for the access, use, and exchange of electronic health data across the European Union. Building on foundational instruments such as the General Data Protection

Regulation (GDPR), the Data Governance Act (DGA), the Data Act, and the NIS2 Directive, the EHDS aims to harmonize both primary and secondary uses of health data, supporting innovation, research, and improved healthcare delivery throughout the EU.
The EHDS is designed to:

- Strengthen individuals' rights by enhancing their access to and control over personal electronic health data.
- Enable the secure and lawful reuse of health data for purposes serving the public interest, such as scientific research, policy development, and innovation.
- Ensure that all data processing occurs within certified secure processing environments, adhering to the highest standards of privacy and cybersecurity.
- Prohibit any attempt to re-identify data subjects when pseudonymised or anonymised data is used for secondary purposes.

The EHDS introduces a multilayered infrastructure and governance model to support both primary and secondary uses of data across the EU. It includes roles for citizens, healthcare providers, data users, and authorities:

- Data Subjects: Individuals who generate and control personal health data, with GDPR rights such as access, rectification, and portability.
- Data Holders: Entities (e.g., hospitals, insurers, EHR providers) are responsible for storing health data and facilitating authorized access.
- Health Professionals: Use data for diagnosis and care under the primary-use pillar, accessing information via MyHealth@EU.
- MyHealth@EU: The EU-wide infrastructure for primary data exchange, supporting ePrescriptions, lab reports, and EHR summaries.
- Health Data Access Bodies (HDABs): National authorities that approve and oversee secondary-use requests, ensuring compliance with EHDS requirements.
- HealthData@EU: A federated platform enabling the sharing of pseudonymised data across borders for secondary use in research, innovation, and policy.
- Secure Processing Environments: Certified infrastructures where secondary data use is conducted, ensuring that data cannot be exported, and all computation remains internal.
- Semantic & Technical Standards: Promote interoperability and data harmonization (e.g., HL7 FHIR, SNOMED CT, ICD-11, eIDAS, LOINC).
- Legal Framework: Ensures all data use is compliant, lawful, and transparent, integrating GDPR, EHDS, Data Act, AI Act, MDR, and NIS2.

The EHDS Regulation entered into force in March 2025. Key rules begin applying in March 2029, with full implementation expected by March 2034, including cross-border data exchange and secondary use across the EU.

Further information on European Health Data Space (EHDS) is available at the following source: European Health Data Space Regulation (EHDS) - Public Health.

3.3 EU Artificial Intelligence Act (EU AI ACT)

The EU Artificial Intelligence Act (AI Act) applies to the deployment of various AI systems and general-purpose AI models within the European Union. It does not, however, apply to the research, testing, or development phases of such systems and models. If a product includes artificial intelligence, it must be assessed under the EU AI Act to determine whether it qualifies as a high-risk system or falls into another category.

Providers of high-risk AI systems must comply with a range of obligations, including:

- Risk Management (Article 9): Establish and maintain a comprehensive risk management system throughout the lifecycle of the AI system.
- Data Governance (Article 10): Use high-quality training, validation, and testing datasets that are relevant, representative, and free of errors and bias.
- Technical Documentation and Logging (Articles 11–12): Maintain detailed technical documentation and implement logging capabilities to ensure traceability and accountability.
- Transparency and User Information (Article 13): Ensure that the system is transparent and that users are provided with clear, understandable information about its functioning and limitations.
- Human Oversight (Article 14): Design the system to allow for effective human oversight, either built into the system or implemented by the user.
- Accuracy, Robustness, and Cybersecurity (Article 15): Guarantee that the system performs reliably and securely, minimizing risks of malfunction or misuse.
- Quality Management System (Article 17): Implement a structured quality management system to ensure ongoing compliance with the regulation.

If a provider determines that their AI system does not pose a significant risk (as outlined in Article 6(2)(a)), they must:

- Registration (Article 49(1)(a)): Register the system in the EU database before placing it on the market or putting it into service.
- Documentation (Article 6(2)(b)): Document the risk assessment and make this documentation available to the National Competent Authorities (NCA) upon request.

If a market surveillance authority later determines that the system was misclassified (Article 80), the provider will be required to comply with the full set of high-risk obligations under Chapter III, Section 2, and may be subject to penalties under Article 99.

Regardless of risk classification, all AI systems must meet transparency obligations. This includes informing individuals in a timely and clear manner when they are interacting with an AI system—unless it is obvious from the context.

The EU AI Act began applying in February 2025, starting with banned systems and AI literacy rules. Key obligations roll out through 2025, with full enforcement for high-risk systems by August 2026. Sector-specific rules follow in August 2027.

More information can be found from the dedicated EU Artificial Intelligence Act website, which provides summaries, implementation timelines, and access to the full legislative text: https://artificialintelligenceact.eu/.

3.4 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) (EU) 2016/679 governs the processing of personal data within the European Union. It applies directly to medical software and digital health solutions, particularly when handling sensitive health-related data.

Key Requirements:

- Lawful basis for processing: Personal data must be processed on valid legal grounds, typically for purposes related to medical diagnosis, treatment, or care. Consent alone is not always sufficient.
- Data minimization: Only data that is strictly necessary for the intended medical or operational purpose may be collected and processed.

- Transparency: Individuals must be clearly informed about how their personal data is collected, used, stored, and protected.
- Data subject rights: Individuals have the right to access, rectify, restrict, or request the erasure of their personal data under certain conditions.
- Security measures: Appropriate technical and organizational safeguards must be implemented, such as encryption, access controls, and secure storage.
- Data Protection Impact Assessment (DPIA): A DPIA is mandatory for high-risk processing activities, including the use of AI in healthcare contexts.
- Purpose limitation: Personal data must be used only for specific, explicit, and legitimate purposes as originally defined.
- Accountability principle: Data controllers must be able to demonstrate compliance with GDPR through proper documentation and internal processes.
- Data breach notification: In the event of a personal data breach, the relevant supervisory authority must be notified within 72 hours.

The GDPR was adopted on April 14, 2016, and entered into force on May 24, 2016, and became fully applicable across the EU on May 25, 2018. From that date, organizations were required to comply with.

Further information on General Data Protection Regulation (GDPR) is available at the following source: Data protection - European Commission.

3.5 Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for all products with digital elements, including software, throughout their entire lifecycle. These requirements aim to ensure that digital products placed on the EU market are secure by design and remain so through regular updates and risk management. If a product requires CE marking, the upcoming CRA must also be taken into account as part of the conformity assessment process. The CRA establishes minimum cybersecurity requirements for devices and software that contain a digital element and are capable of being directly or indirectly connected to another device or to a network. However, the Regulation does not apply to certain categories of products that are already subject to sector-specific cybersecurity requirements. These include, for example, medical devices and in vitro diagnostic medical devices.

The Cyber Resilience Act entered into force on January 22, 2025. Main obligations apply from December 11, 2027, though some take effect earlier during the transition period.

Further information on Cyber Resilience Act (CRA) is available at the following source: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

3.6 Network and Information Security Directive 2 (NIS2)

The NIS2 Directive (EU 2022/2555) strengthens cybersecurity obligations across critical and important sectors, including healthcare, medical devices, and digital infrastructure. It may also apply to AI-based medical software, depending on the provider’s role and classification. NIS2 applies to entities designated as “essential” or “important” within critical sectors. This includes healthcare providers, health IT service providers, medical laboratories, and software vendors that support critical services. Whether an AI-based medical software

provider falls under the scope of NIS2 depends on several factors, such as the size of the organization (typically medium or large enterprises), its role in national healthcare or digital service delivery, and its designation by national authorities. Each EU Member State is responsible for identifying and designating which entities are subject to NIS2 obligations. To maintain compliance, regular audits are required to ensure that products and services continue to meet the directive's cybersecurity requirements. In addition, organizations may pursue recognized cybersecurity certifications, such as ISO/IEC 27001, to demonstrate their commitment to security and regulatory compliance with partners and customers.

The NIS2 Directive entered into force on January 16, 2023. It became applicable on October 18, 2024, following the transposition deadline. Member States had to identify essential entities by April 17, 2025, with the first Commission review set for October 18, 2025.

A comprehensive overview of the directive, including its objectives, scope, implementation requirements, and sectoral coverage, is available on the European Commission's Digital Strategy portal: NIS2 Directive – Shaping Europe's Digital Future [digital-st....europa.eu].

3.7 Medical Device Regulation (MDR)

All medical device regulations are fundamentally based on the ISO 13485 standard, which is the internationally recognized framework for quality management systems in the design and manufacture of medical devices. If a system is classified as a medical device, falling under Class I, IIa, IIb, or III, the requirements of the Medical Device Regulation (MDR) must be followed. Software is considered a medical device if its intended use aligns with the definition provided in the MDR. According to the regulation, a medical device includes any instrument, apparatus, appliance, software, implant, reagent, material, or other article intended by the manufacturer to be used, alone or in combination, for human beings for specific medical purposes such as:

- Diagnosis, prevention, monitoring, prediction, prognosis, treatment, or alleviation of disease;
- Diagnosis, monitoring, treatment, alleviation of, or compensation for an injury or disability;
- Investigation, replacement, or modification of the anatomy or of a physiological or pathological process or state;
- Providing information by means of in vitro examination of specimens derived from the human body, including organ, blood, and tissue donations.

The regulation specifies that such devices do not achieve their principal intended action by pharmacological, immunological, or metabolic means, although they may be assisted in their function by such means. Additionally, the following are also considered medical devices:

- Devices intended for the control or support of conception;
- Products specifically intended for cleaning, disinfection, or sterilization of the above-mentioned devices.

A product is considered compliant when it meets the general safety and performance requirements outlined in Annex I of the MDR. The final product must bear the CE marking as proof of conformity. Furthermore, both the product and its manufacturer must be registered in the EUDAMED database.

The MDR entered into force on May 25, 2017, with a transition period until May 25, 2021. Due to COVID-19, its full application was delayed by one year and took effect on May 26, 2022.

Further information on Regulation on medical devices is available from the official EUR-Lex portal: https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng.

4 Use Case Specific Ethical and Legal Considerations

4.1 Use Case 1: Smart alarm response and context-aware information management

Use Case 1 (UC1) introduces an AI-driven alarm response system that processes real-time patient and staff data to interpret alerts and route them to the most appropriate caregiver. This system touches upon multiple ethical and legal principles as outlined in Chapters 2 and 3 and will be discussed in more detail below.

4.1.1 UC1 Ethical considerations

The European Commission's Ethics Guidelines for Trustworthy AI

Human Agency and Oversight

The system enhances traditional alarm management in hospitals by assigning a priority class to each alert, enabling nurses to respond more efficiently. While the tool presents AI-generated recommendations, nurses retain full control over how alarms are handled. They can review, adjust, or override the suggested priority based on their own assessment of the situation. This approach safeguards nurses' autonomy throughout the decision-making process.

One of the tools will record the voice of the patient (only after an alarm was triggered by pushing a button), derive the patient need and classify the alarm. For this voice-based alarm classification, the original voice records can be made available until the alarm has been completely handled. This enables the nurses to listen to the request of the patient and easily override the suggested priority based on their professional judgment.

As the use case is intended to train the AI model rather than validate its application, it is essential that nurses remain aware of potential error margins and exercise critical judgment in their decision-making. This will be an important focus point during the nurses' training.

Technical Robustness and Safety

Since the system may influence decisions with direct impact on patient care (e.g., when a high priority alarm is incorrectly predicted as low priority), robustness is critical. Thorough validation of the AI models, fallback mechanisms and continuous monitoring are in place to prevent errors such as misinterpretation of alerts. For example, nurses can provide feedback on the AI-suggested priority level of each alert via the app directly. Regular analysis of this feedback helps to identify biases and errors in the model. In addition, if an alert assigned to a caregiver is not addressed within a predefined timeframe, the system automatically escalates the call to another available staff member, ensuring timely response and patient safety. The AI model is only implemented on "normal" patient alerts, not on critical calls such as monitoring or reanimation alarms.

To ensure high-quality care during the pilot phase, new phones will be introduced in the participating department(s) at least a few months before the pilot begins. This approach allows nurses to become familiar with the devices prior to using the app, thereby promoting seamless integration of the app into their daily routines.

Privacy and Data Governance

The project was submitted to the Data Access Committee (DAC) via an online form. The Greenhouse, an internal team within the hospital, manages the subsequent processing of the dossier. This team validates the submission, assigns a specific internal tracking number, and prepares the dossier with all relevant details (including project information, contact details, involved departments, GDPR considerations, and financial aspects) before presenting it to the DAC.

The DAC—comprising the Data Protection Officer (DPO), legal experts, Ethics Committee representatives, physicians, and hospital management—conducted a thorough review of the UC1 process, which involves handling sensitive data such as medication records, patient location, and admission details. Their assessment focused on balancing the operational requirements of the project with strict compliance to privacy regulations and ethical standards. The committee evaluated whether each data element was essential for the intended purpose, assessed potential risks of misuse or re-identification, and verified that appropriate safeguards were in place.

Following this review, the DAC approved the use of the respective data types, based on a detailed justification regarding their intended purpose and handling. If anonymous data are expected, the DAC ensures the effective anonymity of the data provided. If pseudonymous data are expected, the DAC and/or the DPO oversee the necessary measures to ensure compliance with GDPR requirements. Finally, a Data Transfer Agreement is established with the parties involved. Through the hospital's privacy statement, patients are informed that sensitive health data may be processed for secondary purposes.

Transparency and Explainability

Prior to implementing the system within the hospital, nurses and other personnel receive comprehensive training covering both the practical use of the app and the underlying AI functionalities. This ensures that staff understand not only how to operate the system, but also how the AI supports their decision-making.

In terms of explainability, the app displays key points for each patient, such as pain score, increased fall risk, or physical restraint measures. By making these factors visible, the system offers valuable insight into why a particular alert was classified at a certain priority level.

Diversity, Non-Discrimination and Fairness

The AI model must avoid bias that could lead to unequal treatment of patients or staff. To achieve this, the model is trained on diverse datasets that include a wide range of patient profiles (e.g. geriatric wards, maternity, regular wards). Additionally, end-users (nurses, care assistants, managers, etc.) from different wards are actively involved in the design process through workshops and feedback sessions, ensuring that the system reflects the needs and perspectives of all groups.

Societal and Environmental Well-being

In hospitals, a significant amount of time is wasted in poor management of information and unplanned care services caused by a variety of alarms. Typically, information is difficult to acquire at the point of decision-making; hence, it is challenging to have the right resources in the right place at the right time to efficiently meet care needs. By enabling a more efficient scheduling and assignment of alerts, UC1 contributes to faster care delivery and reduced staff workload, thereby improving care quality and patient well-being.

Adherence to the Declaration of Helsinki and Research Ethics Governance

Adherence to the Declaration of Helsinki and research ethics governance in UC1 is ensured through a rigorous process that begins with submission of the study protocol – detailing the types of data that will be used, what they will be used for and how pseudonymization is applied – to the hospital's data access committee for approval before any patient or staff data is processed. In the next stage, when the AI-supported alarm system is piloted in the hospital, approval from the hospital's ethics committee will be obtained and staff and patients will be fully informed about the study's purpose and how their information will be used.

The Ethics Committee will review the study protocol and evaluate the associated documents for compliance with GDPR requirements and the Clinical Trials Act. The committee will provide feedback to the project team and request revisions to the documents as needed. Following Ethics Committee approval, the project will be monitored internally by a dedicated study team trained in the study protocol and Good Clinical Practice (GCP) guidelines. The Ethics Committee will remain available to address any questions throughout the study. The informed consent process will be conducted in accordance with the hospital's standard operating procedures.

4.1.2 UC1 Legislative considerations

Data Governance Act (DGA)

The Data Governance Act (DGA) may be relevant to UC1 only if data is reused or shared beyond its original clinical purpose and context. In the current setup, patient-related alarm data and associated workflow metadata may be shared between the hospital and Televic (the technology partner) for the purpose of improving AI models used in UC1. However, since this data sharing remains within a bilateral processor–controller relationship, is governed by a GDPR-compliant contract (Article 28), and is not shared with third parties or repurposed for general use, it is unlikely to fall under the DGA's broader obligations related to data intermediation or data altruism.

Thus, the system should ensure:

- Proper role and purpose specification in the processor agreement,
- Data pseudonymisation or anonymisation where feasible,
- Clear documentation of how model training aligns with the original purpose of care delivery.

EU Artificial Intelligence (AI) Act

UC1 might qualifiy as a high-risk AI system due to its role in healthcare decision support under the AI Act, particularly under Annex III, point 5(a), which includes AI systems used in healthcare to support decisions that may affect patients' health. While UC1 does not make

autonomous medical decisions, its real-time alarm triage and prioritization mechanisms directly influence how quickly nurses respond to alarms, thus potentially affecting patient outcomes.

The classification is not automatic simply because the system is used in healthcare; rather, it depends on whether:

- The AI influences clinical decision-making;
- The decision could have a significant impact on health or safety.

In UC1, both conditions are met, justifying its classification as high-risk.
Consequences of being high-risk include:

- Risk management system and documentation (Article 9–10);
- Data governance and bias mitigation;
- Human oversight and explainability (Article 14);
- Conformity assessment and registration.

Therefore, UC1 developers and deploying hospitals should begin aligning with AI Act obligations. Formal compliance with the AI act is out of scope for this project.

General Data Protection Regulation (GDPR)

UC1 involves the real-time processing of sensitive personal data in a healthcare context, including alarm signals linked to patient status, contextual information from electronic health records (EHR), staff shift and location data, and care coordination metadata. This processing falls under the GDPR and is governed by multiple articles related to special category data, security, lawful basis, and risk mitigation.

<u>Legal Basis for Processing</u>
The primary lawful bases applicable to UC1 are:

- Article 6(1)(e): Processing is lawful when it is necessary for the performance of a task carried out in the public interest.
- Article 9(2)(h): Processing of special category data (such as health data) is permitted when necessary for the provision of health or social care, including care coordination and management of healthcare systems.

These provisions permit the operation of alarm triage and context-aware support systems without requiring explicit consent, provided adequate safeguards are in place, such as data minimization, access control, encryption, transparency to staff and patients, and the completion of a Data Protection Impact Assessment (DPIA).

<u>Core GDPR Principles (Article 5)</u>
UC1 must adhere to the fundamental GDPR principles, including:

- Lawfulness, fairness, and transparency (Art. 5(1)(a)): Data subjects (staff and, where relevant, patients) must be informed about the processing activities, including purposes and rights.
- Purpose limitation (Art. 5(1)(b)): Data must be collected for clearly defined clinical purposes and not repurposed without appropriate legal basis.
- Data minimization (Art. 5(1)(c)): Only data necessary for alarm prioritization and care coordination should be processed.
- Accuracy (Art. 5(1)(d)): Data inputs such as staff location, patient condition, and alarm states must be current and reliable.
- Storage limitation (Art. 5(1)(e)): Alarm data and related logs must not be retained longer than necessary for clinical use or auditing.

- Integrity and confidentiality (Art. 5(1)(f), Art. 32): Strong technical and organizational measures, such as encryption, access control, and secure logging, are required to protect data from unauthorized access or breach.

Records and Accountability (Articles 24, 28–30)

- The healthcare institution deploying UC1 is the data controller, responsible for GDPR compliance under Article 24.
- Any service or technology provider supporting system operation acts as a data processor, requiring a binding contract under Article 28.
- A Record of Processing Activities (ROPA) must be maintained as per Article 30, detailing the purposes, data categories, recipients, and retention periods.
- Access to the system must be governed by access controls aligned with Article 29, and all processing activities must be logged and auditable.

Data Subject Rights and Transparency (Articles 12–21)

Even under the healthcare exemption (Art. 9(2)(h)), data subject rights remain applicable:

- Transparency (Art. 13/14): Staff and patients must be informed about the nature, scope, and safeguards of data processing.
- Access and rectification (Art. 15/16): Staff should be able to review and correct data related to their profiles, locations, and assigned tasks.
- Restriction and objection (Art. 18/21): Where applicable, individuals may object to certain forms of secondary use or profiling not directly linked to care provision.

Limitations to these rights may apply in accordance with Article 23, but only if justified under national healthcare regulations.

DPIA and Risk Assessment Obligations

Due to the high sensitivity of the data and the system's potential to affect real-world clinical decisions, a Data Protection Impact Assessment (DPIA) is mandatory under Article 35 GDPR. This DPIA must assess risks to the rights and freedoms of individuals and define mitigation strategies, particularly around:

- Misclassification of alarms
- Unauthorized access to location or health data
- Secondary uses of data beyond clinical care

Cyber Resilience Act (CRA)

The CRA imposes cybersecurity requirements on all digital products with connectivity features. It applies to software and hardware placed on the market outside the scope of sectoral regulations like the MDR.

In UC1, parts of the system (e.g., alarm middleware, location tracking software, interfaces) are not considered medical devices but are network-connected and deployed in healthcare infrastructure, therefore they fall under the CRA.

The CRA principles, such as secure-by-design development, patch management, and incident reporting, are good practice in UC1 due to the sensitivity and operational criticality of healthcare alarms.

Network and Information Security Directive 2 (NIS2)

NIS2 expands the scope of cybersecurity regulation to cover more sectors, including healthcare service providers. Since UC1 is deployed in a hospital or care facility designated as an "essential entity" under NIS2, the system becomes part of critical infrastructure.

This triggers legal obligations on the organization hosting UC1 to:

- Implement cybersecurity risk management policies;
- Establish robust incident response and reporting procedures;
- Enforce technical and organizational security measures;
- Conduct audits and ensure staff cybersecurity training.

Even if the hospital is not formally covered by NIS2, adopting its principles (e.g., access control, monitoring, traceability, data recovery plans) supports resilience and may align with institutional requirements for IT governance and digital health certification.

4.1.3 UC1 Special considerations

UC1 operates within key Belgian ethical and legislative frameworks, such as the Law on Patients' Rights and the (Healthcare Practice) Quality Act. Core requirements, such as GDPR compliance, the EU AI Act, transparency, and continuous oversight, detailed in chapters 4.1.1 and 4.1.2, are fully addressed in the system's design. Specifically, UC1 upholds the principles of the Patients' Rights Act by ensuring patients receive clear information about data usage and have opportunities to provide informed consent where necessary. In line with the Quality Act, UC1 integrates structured quality assurance measures, such as ongoing monitoring and comprehensive logging, to support safe, high-quality care and accountability.

4.2 Use Case 2: Deployment of AI-enabled solutions into clinical practice

Use Case 2 (UC2) focuses on the deployment of AI-enabled solutions into clinical practice. Central to this effort is the development of a highly performant compute platform designed to host a range of surgical AI applications capable of processing real-time video streams over IP. These applications aim to support intraoperative decision-making by providing intelligent overlays on top of the video streams and insights during surgical procedures.

To ensure safe and reliable operation throughout the lifecycle of these AI applications — including deployment, shadow monitoring, and post-market follow-up — a dedicated Quality Assurance (QA) layer is being developed. This layer continuously monitors both the performance of the compute platform and the behavior of the deployed AI models, enabling intervention when quality or safety thresholds are compromised.

In the following sections, we outline the ethical and legislative considerations relevant to the UC2 compute platform and QA layer. We highlight or contrast specific elements discussed in Sections 2 and 3 to provide an overview of the regulatory and ethical considerations.

4.2.1 UC2 Ethical considerations

Human Agency and Oversight

In UC2, the compute platform must incorporate a manual override mechanism that allows surgeons to disable AI-generated overlays at any moment. This safeguard ensures that clinicians retain full control over the information presented during procedures. While the specific input device used to trigger this override falls outside the scope of the PROFIT project, its integration into the clinical workflow is essential.

Beyond manual control, the QA layer will continuously monitor the performance of both thecompute platform and deployed AI applications to detect when the quality of service deteriorates below acceptable thresholds. In such cases, the system may initiate an automatic override, temporarily disabling AI overlays to prevent potentially misleading or low-confidence information. The exact parameters and decision logic for this automatic intervention are still under development.

Technical Robustness and Safety

In UC2, AI applications undergo a multi-phase validation process prior to deployment. This includes:

- Installation Qualification: Verifying that the system and hardware are correctly installed according to specifications.
- Operational Qualification: Confirming that the system operates as intended under expected conditions.
- Performance Qualification: Demonstrating that the AI application performs reliably and accurately in the clinical environment.

Following deployment, a shadow monitoring phase is initiated. During this phase, the AI application is executed on-site using real-world input data, but without influencing clinical

decision-making. This allows for performance evaluation under authentic conditions while preserving patient safety and clinician autonomy.

Once the AI application is fully integrated into clinical workflows, post-market follow-up mechanisms are activated. These include:

- Version control and rollback mechanisms, enabling safe reversion to previous model versions if performance issues arise.
- Adverse event reporting, allowing clinicians and stakeholders to document and respond to unexpected outcomes or system failures.
- Re-validation of updated models, ensuring that any new AI versions meet the same rigorous standards as the original deployment.

Together, these measures contribute to a technically robust and safe AI ecosystem, aligned with the principles of the EU AI Act and ISO standards for medical device software. The QA layer within UC2 plays a central role in this lifecycle management, enabling continuous performance tracking and detection of anomalies that may compromise safety or reliability.

Privacy and Data Governance

In UC2, sensitive patient data may be processed. This may involve identifiable video streams or Electronic Health Records (EHRs) which may be processed alongside the surgical video feeds. Privacy and data governance need to be taken by heart, and robust safeguards must be put in place to ensure compliance with the General Data Protection Regulation (GDPR). To mitigate privacy risks, data minimization and anonymization strategies will be applied wherever possible. For instance, identifiable elements in surgical video streams will be anonymized prior to processing, and aggregated data will be used for performance analysis and model improvement.

Furthermore, the UC2 compute platform will be designed in accordance with privacy-by-design and privacy-by-default principles. This includes:

- Limiting access to personal data to only what is strictly necessary for the intended clinical or QA purpose.
- Embedding data protection mechanisms into the architecture of the compute platform and AI applications.
- Ensuring that data processing activities are transparent, auditable, and subject to appropriate access controls.

The QA layer also contributes to privacy governance by enabling traceability and accountability across the AI lifecycle. It ensures that data used for monitoring and post-market follow-up is handled in a secure and compliant manner, and that any updates to AI models are subject to renewed privacy assessments.

Transparency and Explainability

In UC2, transparency and explainability are addressed by ensuring that both clinicians and patients are adequately informed about the role and functioning of AI during surgical procedures. Specifically, clear and accessible explanations regarding the real-time analysis performed on surgical video feeds, including the nature of AI-generated overlays and how they contribute to clinical decision-making, must be provided.

To support traceability and accountability, the compute platform will maintain immutable logs of all system activities. These logs enable auditability and support post-market surveillance. Moreover, they contribute to regulatory compliance under frameworks such as the EU AI Act, which mandates transparency in high-risk AI systems.

Explainability also extends to the design of the user interface and interaction mechanisms. Wherever feasible, the system should provide contextual cues or confidence indicators to help clinicians interpret AI outputs. While full interpretability may not be achievable for deep learning models, efforts should be made to ensure that the system's behaviour is predictable, understandable, and justifiable in the clinical context.

Diversity, Non-Discrimination and Fairness

In UC2, diversity and fairness are addressed through both pre-deployment documentation and ongoing performance auditing.

Before an AI application is deployed on the compute platform, developers are required to submit an application card or model card. This documentation must include:

- A description of the training data used, including demographic composition,
- The intended clinical use and context,
- Known limitations or performance caveats.

Currently, there is no EU-mandated repository for model cards under the AI Act or MDR. Model cards can thus be submitted at different levels. Firstly, many healthcare organisations require model cards to be submitted to their internal AI governance or clinical technology bodies. These bodies then perform an internal review in terms of transparency, bias, clinical relevance, fairness, safety, and so on. Secondly, if the UC2 compute platform would qualify as a medical device (see Section 4.2.2 EU AI Act and MDR for this discussion), then model cards can become part of the technical documentation required for MDR. The review of these model cards would then happen at the regulatory level and be performed by a notified body. Finally, industry initiatives like the Coalition for Health AI (CHAI) Model Card Registry can be considered as well. The CHAI registry does not validate model cards in any way but provides a centralized repository for health AI model cards and ensures standardized formatting and completeness. The aim of submitting model cards to an industry repository like CHAI is to support transparency and benchmarking across institutions.

This process promotes transparency and accountability, ensuring that models are not only technically robust but also ethically sound. It also helps identify potential biases early in the deployment pipeline.

To monitor the fairness of deployed AI applications during real-world use, the QA layer includes a dedicated bias monitoring module. This component performs demographic performance audits, evaluating how the AI model performs across different subpopulations. If disparities are detected, corrective actions can be taken, such as notifying the AI vendor for model retraining, threshold adjustments, or temporary deactivation of the application.

These mechanisms support compliance with the EU AI Act's requirements for high-risk AI systems, which mandate fairness, non-discrimination, and mitigation of bias.

Societal and Environmental Well-being

AI systems deployed in clinical practice should contribute positively to society and minimize their environmental footprint. In UC2, societal well-being is supported by the overarching goal of enhancing surgical precision, improving patient outcomes, and reducing variability in clinical decision-making. By integrating AI into real-time surgical workflows, UC2 aims to augment human expertise, reduce cognitive load, and support safer, more efficient procedures — ultimately benefiting both patients and healthcare professionals.

The QA layer further contributes to societal well-being by enabling continuous monitoring, feedback, and accountability, ensuring that AI systems remain safe, effective, and aligned with clinical needs throughout their lifecycle.

From an environmental perspective, the UC2 compute platform is designed with resource efficiency in mind. Rather than deploying multiple specialized devices on individual trolleys per operating room (OR), a single compute unit is capable of serving multiple ORs simultaneously and hosting a wide variety of AI applications. This consolidated architecture reduces hardware redundancy, lowers energy consumption, and simplifies maintenance. It also supports scalability and flexibility, allowing hospitals to expand their AI capabilities without a proportional increase in physical infrastructure.

4.2.2 UC2 Legislative considerations

Data Governance Act (DGA)

The Data Governance Act (DGA) provides a framework for secure and trustworthy data sharing across the EU, particularly when data is reused beyond its original purpose or shared with third parties. UC2 may fall under the scope of the DGA only if data collected during clinical use — such as surgical video recordings or derived metadata — is shared externally for secondary purposes, such as research, commercial reuse, or public data spaces.

At present, such redistribution is not foreseen, and data remains within the clinical context. Therefore, the DGA is not currently applicable to UC2. However, this status may change if future use cases involve broader data sharing or participation in EU-wide health data spaces.

European Health Data Space (EHDS)

The European Health Data Space (EHDS) aims to facilitate secure and interoperable access to health data across the EU for both primary and secondary use. Its primary focus is on empowering individuals with control over their health data and enabling data sharing for research, innovation, and policymaking.

UC2 is currently not within the scope of EHDS, as it does not involve cross-border data sharing or participation in EU-wide health data infrastructures. All data processing remains local to the clinical institution, and there are no plans at this stage to contribute data to EHDS-related initiatives.

However, future integration with EHDS may become relevant if UC2 evolves to support broader data sharing for research or public health purposes. In such cases, compliance with EHDS requirements — including interoperability standards, patient consent mechanisms, and data access governance — would need to be reassessed.

EU Artificial Intelligence (AI) Act & Medical Device Regulation (MDR)

The deployment of AI-enabled systems in clinical practice, such as the UC2 compute platform, requires careful consideration of both the EU Artificial Intelligence Act (AI Act) and the Medical Device Regulation (MDR). These two legislative frameworks operate in parallel and are complementary, not mutually exclusive. If the compute platform is classified as a medical device under MDR, it will automatically be considered a high-risk AI system under the AI Act.

At present, it remains unclear whether the UC2 compute platform qualifies as a medical device. This determination depends on its intended medical purpose, whether it influences clinical decisions, and whether it meets the definition of Medical Device Software (MDSW). If classified as such, UC2 would be subject to a dual compliance regime, requiring conformity with both MDR and the AI Act.

In the event that the compute platform is considered a medical device, the following AI Act obligations for high-risk systems would apply:

- Risk Management System: Continuous and iterative risk assessment across the AI lifecycle, including deployment, monitoring, and updates.
- High-Quality Data: Use of representative, relevant, and bias-mitigated training, validation, and testing datasets.
- Technical Documentation & Logging: Comprehensive documentation of system design, performance, and decision logic, along with immutable logs of system activity.
- Transparency & User Information: Clear communication of system capabilities, limitations, and intended use to clinicians and other users.
- Human Oversight: Built-in mechanisms for manual override and safeguards to ensure clinicians can intervene or contest AI outputs.
- Accuracy, Robustness & Cybersecurity: Measures to ensure reliable performance under expected conditions and protection against adversarial threats.
- Quality Management System (QMS): Integration of AI-specific controls into the existing MDR-compliant QMS, covering data governance, bias monitoring, and post-market surveillance.

The QA layer within the compute platform is well-positioned to support many of these requirements, particularly in areas such as performance monitoring, logging, and bias auditing.

General Data Protection Regulation (GDPR)

Compliance with the General Data Protection Regulation (GDPR) is essential for UC2, given its potential to process sensitive patient data, including surgical video streams and Electronic Health Records (EHRs). GDPR governs the lawful, fair, and transparent processing of personal data within the EU, and applies to both clinical use and any secondary data sharing activities.

UC2 must adhere to the following core GDPR principles:

- Lawful Basis: Data processing must be grounded in a valid legal basis, such as patient consent, legitimate interest, or performance of a medical task.
- Data Minimization: Only data strictly necessary for the intended purpose should be collected and processed.

- Purpose Limitation: Data must be used solely for the purposes explicitly stated at the time of collection.
- Transparency: Patients and clinicians must be informed about how data is processed, stored, and potentially shared.
- Data Subject Rights: Mechanisms must be in place to support rights such as access, rectification, erasure, and objection.
- Security Measures: Appropriate technical and organizational safeguards must be implemented to protect data from unauthorized access or breaches.

A Data Protection Impact Assessment (DPIA) must be conducted prior to deployment, especially given the scale and sensitivity of data processing in surgical environments.

Importantly, if performance data, logs, or feedback from deployed AI models — particularly if linked to identifiable patient information or clinical context — are shared with the original AI vendors, this activity falls under the scope of GDPR. In such cases:

- The clinical institution typically acts as the data controller, while the vendor may be a data processor or a joint controller, depending on the contractual arrangement.
- A Data Processing Agreement (DPA) must be established to define roles, responsibilities, and safeguards.
- Shared data should be anonymized or pseudonymized where possible to reduce privacy risks.
- The sharing must be transparent to data subjects, and consent may be required depending on the nature of the data and its intended use.

Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA) establishes mandatory cybersecurity requirements for products with digital elements that are made available on the EU market. Its goal is to ensure that such products are secure throughout their lifecycle — from design and development to maintenance and decommissioning.

However, UC2 is exempt from the CRA if the compute platform is classified as a medical device under MDR. The CRA explicitly excludes products that fall under existing sector-specific regulations, including medical devices.

If the compute platform is not considered a medical device, then it may fall under the CRA's scope as a connected product with digital elements. In that case, it would need to comply with cybersecurity obligations such as:

- Secure-by-design principles,
- Vulnerability management and patching,
- Lifecycle documentation and attestation,
- CE marking to demonstrate conformity.

Given the current uncertainty around UC2's classification, the applicability of the CRA should be reassessed once the MDR status is clarified.

Network and Information Security Directive 2 (NIS2)

The applicability of NIS2 to UC2 must be carefully assessed. The directive applies to any digital system supporting critical services — particularly those involved in healthcare delivery, data processing, or infrastructure management. If the compute platformis deployed

in a way that supports or enables critical clinical operations, such as real-time surgical decision support or video routing in operating rooms, it may be considered part of the essential digital infrastructure of the hospital.

Key indicators for NIS2 applicability include:

- Operational criticality: Does the compute platform support services whose disruption would significantly impact patient care?
- Data sensitivity: Does it process or transmit sensitive patient data?
- Organizational size and role: Is the deploying institution classified as a medium or large healthcare provider under NIS2 thresholds?

If deemed in scope, UC2 would need to comply with NIS2 obligations, including:

- Implementing technical and organizational cybersecurity measures,
- Conducting regular risk assessments and penetration testing,
- Ensuring incident reporting within 24 hours of detection,
- Maintaining business continuity and recovery plans,
- Assigning clear accountability for cybersecurity at the management level.

Given the potential classification of UC2 compute platform as a critical digital system in healthcare, a formal risk assessment and legal review should be conducted to determine its status under NIS2.

4.2.3 UC2 Special considerations

Beyond the ethical and legislative frameworks discussed in Chapters 2 and 3, UC2 also aligns with emerging international best practices and global initiatives that promote responsible AI in healthcare. Notably, UC2 is being developed in accordance with:

- Good Machine Learning Practice (GMLP) guidelines, which emphasize robust data management, reproducibility, and continuous performance monitoring across the AI lifecycle.
- Recommendations from the WHO-ITU Focus Group on AI for Health (FG-AI4H), which advocate for transparency, equity, and safety in AI systems deployed in clinical settings.

These frameworks provide valuable guidance for the design, validation, and governance of AI-enabled surgical support tools, especially in complex, real-time environments.

In addition, UC2 anticipates the need to support adaptive AI systems — models that evolve over time through mechanisms such as federated learning or continuous retraining. To manage such evolution responsibly, the concept of Predetermined Change Control Plans (PCCP) is applied. PCCPs define pre-approved modifications to AI models based on real-world learning, ensuring that updates remain within validated boundaries and do not compromise safety or performance.

The QA layer plays a central role in enabling adaptive AI. Through its integrated monitoring, logging, versioning, and validation functionalities, it supports the implementation of PCCPs and ensures that model updates are traceable, auditable, and compliant with regulatory expectations.

4.3 Use Case 3: Real-time asset tracking and sterilization management system for the safe reuse of invasive medical diagnostic equipment

Use Case 3 (UC3) focuses on management of reusable invasive medical diagnostic equipment in a gastroenterology unit at Portuguese hospital setting. To evaluate unavailability periods and causes, equipment lifecycle will be analyzed, including usage, decontamination procedures, microbiological testing and maintenance/repairing aiming to identify bottlenecks, propose metrics for operational efficiency, and suggest data-informed improvements for smart hospital logistics. The analysis covers usage patterns and equipment unavailability periods; decontamination and sterilization workflows; microbiological testing and validation; and maintenance and repair cycles.
The aim is to identify process constraints, define operational performance metrics, and propose data-informed optimizations that enhance safety and sustainability.
UC3 contributes to safer hospital logistics by ensuring that equipment reuse complies with infection control protocols, European data governance standards, and national health regulations.

4.3.1 UC3 Ethical considerations

UC3 prioritises operational ethics, focusing on patient and staff safety, traceability, and responsible data use. While Chapter 2 addresses ethics in AI-driven and data-intensive systems, UC3 emphasises human responsibility, procedural safety, and accountability in equipment management. The key ethical principles which apply are:

- Transparency – Stakeholders are informed about data collection and operational use.
- Proportionality and minimisation – Data processing is limited to operational necessity.
- Safety and non-maleficence – Equipment reuse occurs only after validated decontamination and microbiological control.
- Accountability – Institutions ensure ethical governance throughout the data lifecycle.
- Professional integrity – System use respects healthcare professional ethical codes.

Ethical risks and mitigation strategies planned by US3 are summarized in Table 1.

Table 1. Ethical Risks and Mitigation Strategies.

Ethical Aspect	Identified Risk	Mitigation Strategy
Data tracking of staff or patients	Risk of indirect identification or surveillance	Pseudonymisation and role-based data access
Equipment reuse decisions	Risk of unsafe or premature reuse	Mandatory microbiological validation before reallocation
Monitoring of staff performance	Potential misuse of operational data	Transparency in purpose; anonymised reporting for management use
Data retention	Excessive storage beyond operational needs	Apply storage limitation principles; define clear retention policy

4.3.2 UC3 Legislative considerations

UC3 operates under a robust legal framework that governs both healthcare equipment management and data protection. Chapter 3 provides a general overview of digital health regulation; UC3 applies these principles concretely within hospital logistics.

Key applicable legal instruments include:

- Cyber Resilience Act (CRA – EU 2024/2847) – Applies to network-connected digital products. Supporting software not covered by MDR may fall under CRA; compliance ensures cybersecurity by design and vulnerability management.
- Data Governance Act (DGA – EU 2022/868) – Relevant if UC3 data are reused externally for research or benchmarking. Introduces data intermediaries and conditions for lawful secondary data use.
- EU Artificial Intelligence Act (AI Act – 2024) – The AI component could be classified as high-risk due to the clinical context. Requires risk management, human oversight, robustness, transparency, and explainability.
- European Health Data Space (EHDS – Proposal COM/2022/197) – Establishes interoperability and security standards for primary and secondary health data. Only pseudonymised or anonymised data may be shared in secure processing environments.
- General Data Protection Regulation (GDPR – EU 2016/679) – Governs processing of personal data. DPIA is mandatory due to the sensitivity of the context. Metadata associated with equipment tracking must be carefully assessed for reidentification risk.
- Medical Device Regulation (MDR – EU 2017/745) – Applies if the system influences clinical workflows or supports decisions on equipment reuse. Requires device classification, CE marking, risk management, and conformity to ISO 13485.
- NIS2 Directive (EU 2023/2555) – Establishes cybersecurity, incident reporting, and governance obligations for essential healthcare entities.
- Portuguese National Legislation – Includes Lei n.º 58/2019 (GDPR adaptation), ERS regulations (quality and safety), and SNS Digital Strategy (interoperability).

Table 2 summarises applicable EU and national frameworks relevant to UC3, their key provisions, and compliance actions.

Table 2. Legal and Ethical Compliance Summary.

Regulation / Framework	Relevance to UC3	Applicable Provisions / Key Requirements	Compliance Actions / Mitigation Measures
GDPR (EU 2016/679)	Core Regulation	Lawful processing of personal and operational data; DPIA; principles of purpose limitation, minimisation, and transparency	Conduct DPIA; define lawful basis; implement pseudonymisation, access control, and transparency notices
Lei n.º 58/2019 (Portugal)	National Implementation	Implements GDPR at national level; oversight by CNPD	Appoint DPO; ensure CNPD compliance; national reporting
MDR (EU 2017/745)	Applicable	Influences clinical workflows; classification, CE marking, ISO 13485	Verify SaMD status; conformity assessment; register in EUDAMED; post-market surveillance

Regulation / Framework	Relevance to UC3	Applicable Provisions / Key Requirements	Compliance Actions / Mitigation Measures
EU AI Act (2024)	Likely High-Risk	Risk classification; human oversight; robustness; transparency	Conduct risk assessment; human-in-the-loop; explainable outputs
CRA (EU 2024/2847)	Conditional	Applies to connected digital products not covered by MDR; cybersecurity principles	Apply MDR cybersecurity practices; integrate ISO 27001/IEC 62443
NIS2 (EU 2023/2555)	Relevant for CHL	Cybersecurity, incident reporting, governance	ISO 27001-aligned policies; incident response plan; IT staff training
EHDS (Proposal COM/2022/197)	Conditional (Secondary Use)	Interoperability and security standards; pseudonymised/anonymised data	Align with HL7 FHIR/SNOMED CT; follow secure access framework
DGA (EU 2022/868)	Conditional	Reuse of anonymised datasets; data intermediaries	Apply if UC3 data reused externally; ensure consent/anonymisation
ERS Regulations (Portugal)	National	Quality and safety; sterilisation performance monitoring	Integrate KPIs; microbiological audits; continuous monitoring
Ethical Standards & Human Oversight	Core Ethical Domain	Fairness, accountability, transparency, human control, protection from discrimination	Enable informed staff participation by providing all relevant information, ethical principles, and human oversight for AI-assisted decisions. This can be achieved through clear documentation of AI systems, accessible ethical guidelines, staff training, transparent explanations of AI-driven decisions, and feedback and oversight channels to ensure responsible human control.

4.3.3 UC3 Special considerations

UC3 aligns with several national and institutional requirements:

- Lei n.º 58/2019 – national GDPR adaptation, overseen by CNPD.
- ERS – quality and safety standards in healthcare, including infection prevention and sterilization/decontamination control.
- SNS Digital Strategy – data interoperability and secure information exchange within the Serviço Nacional de Saúde (SNS).
- Internal hospital protocols – govern decontamination, microbiological testing, maintenance, and incident traceability.

- Use of AI and personal data must respect ethical principles such as transparency, fairness, and patient/staff autonomy. Informed use of decision-support tools, non-discrimination in resource planning, and purpose-limited data usage are required.
- Professional ethical guidelines (e.g., from the Portuguese Ordem dos Médicos and Ordem dos Enfermeiros) also apply.

These frameworks ensure compliance with national regulations and reinforce accountability, traceability, and patient safety in hospital operations.

4.3.4 Summary of Data and Associated Risks

Table 3 summarises UC3 data types, risks, relevant regulations, and mitigation measures.

Table 3. UC3 data types, risks, relevant regulations, and mitigation measures.

Data Type	Main Risks	Relevant Regulations	Controls / Mitigation Actions
Equipment identifier	Indirect linkage to staff/patient procedures	GDPR, MDR	Pseudonymisation; limited access; audit logging
Operator ID	Surveillance or performance inference	GDPR, AI Act, National Ethics Codes	Role-based access; minimal collection; transparency
Equipment location data	Behavioral profiling; sensitive location mapping	GDPR, NIS2	Network segmentation; minimal granularity
Microbiological test data	Reidentification of staff; exposure of QC results	GDPR, MDR, CRA	Secure transmission; encrypted storage; QA controls
Microbiological results (pass/fail)	Incorrect reuse due to false negatives	MDR, AI Act	Human validation; explainable AI logic
AI-generated contamination prediction	Bias or opacity	AI Act, GDPR	Documentation; human-in-the-loop review; interpretability
Operational data reused for research	Reidentification; lack of consent	EHDS, GDPR, DGA,	Anonymisation; ethical board approval; secure environments

4.3.5 Conclusion

UC3 demonstrates a practical approach to hospital asset management, enhancing:

- Patient safety, through validated sterilization and microbiological controls;
- Regulatory compliance, aligning with EU and Portuguese legal frameworks;
- Operational efficiency, via real-time tracking and data-informed logistics;
- Ethical governance, ensuring accountability, transparency, and human oversight.

By integrating real-time asset tracking and validated decontamination workflows, UC3 supports sustainable, data-informed, and safe healthcare management in Portugal.

4.4 Use Case 4: Digital home care and preventive digital care

4.4.1 UC4 Ethical considerations

European Commission's Ethics Guidelines for Trustworthy AI

The European Commission's Ethics Guidelines for Trustworthy AI emphasize human agency, technical robustness, privacy, transparency, diversity, societal wellbeing, and accountability. In UC4, digital home care solutions are specifically designed to respect patient autonomy by ensuring that interventions enhance rather than replace human decision-making. AI algorithms in UC4 are developed with rigorous validation methods to maintain technical robustness and safety, addressing potential errors in remote monitoring proactively.

However, implementing robust privacy and transparency in UC4 poses challenges, particularly due to the sensitive nature of healthcare data. To mitigate this, comprehensive privacy protocols consistent with GDPR requirements, including anonymization and secure data handling practices, are employed extensively. Transparency, another critical ethical element, requires clearly communicating AI-driven decisions to patients in UC4. However, achieving this transparency without overwhelming or confusing elderly users—who might already face cognitive or physical limitations—is a notable challenge that UC4 continuously addresses through intuitive, user-friendly interfaces and communication practices.

Declaration of Helsinki and Medical Ethics

In alignment with the Declaration of Helsinki, UC4 maintains high standards of informed consent. Digital care solutions explicitly communicate potential risks, benefits, and details regarding data usage. Given the diverse demographics typically engaged in digital home care scenarios, achieving truly informed consent in UC4 remains challenging. UC4 proactively tackles this through iterative feedback mechanisms and personalized consent processes, ensuring continued patient understanding and engagement.

UC4 is deeply committed to medical ethics, particularly the principles of non-maleficence and beneficence. Digital interventions in home care scenarios have the potential for direct impact on patient health outcomes; hence, Oiva Health integrates rigorous ethical oversight and clinical validation phases into its development cycles (in adherence to its ISO:13485 certification), by involving social and healthcare experts into the product and service model development processes. This proactive stance ensures interventions align with patient safety and beneficial outcomes, though resource-intensive validation and ethical oversight processes present ongoing operational challenges.

Transparency, Equity, and Patient Autonomy

Transparency in UC4 entails clear explanations about AI-driven recommendations and data handling practices. Ensuring such clarity in a home care context, where patient interaction with technology might be intermittent or limited, is challenging. UC4 actively addresses this through comprehensive education programs for social and healthcare staff via our Knowledge Center that is used for online and live training of all end-user stakeholder groups and continuous user-support systems.

Equity is a cornerstone for UC4, ensuring digital home care solutions are accessible across different patient groups. UC4 prioritizes adaptive technology designs (e.g. ease of use for disabilities, the WCAG requirements and dynamic switching of language support on end-user individual preferences) catering to varied socioeconomic backgrounds, linguistic groups, and digital literacy levels. However, equitable access remains complex due to resource limitations, varying infrastructure quality, and disparities in technological availability.

Patient autonomy within UC4 means empowering patients through clear data sharing options and decision-making authority regarding their care paths. Respecting autonomy is operationalized through intuitive consent mechanisms and clearly documented opt-out pathways, which are essential yet challenging to maintain consistently across different user segments.

4.4.2 UC4 Legislative considerations

Data Governance Act (DGA)

For UC4, compliance with the DGA involves ensuring data sharing standards support secure interoperability between healthcare providers. UC4 specifically incorporates standardized data formats and secure communication channels. For instance, UC4 scenarios involving patient monitoring and alerting systems must securely exchange data between care providers and family members, requiring compliance with standardized data-sharing protocols. However, interoperability challenges arise from legacy systems and varied implementation standards across organizations, complicating real-time data exchanges and necessitating substantial investment in system harmonization and middleware solutions.

European Health Data Space (EHDS)

EHDS compliance within UC4 necessitates seamless data integration and exchange across healthcare organizations and national borders. An example scenario includes cross-border elderly care management, where patient data needs to be securely accessed by healthcare providers in multiple EU countries. UC4 employs standardized interoperability protocols (HL7, FHIR), but practical implementation is complicated by national differences in data privacy laws and digital infrastructure capabilities, requiring considerable coordination and harmonization efforts.

EU AI Act (EU Artificial Intelligence Act)

UC4, classified as a high-risk healthcare application under the EU AI Act, faces stringent compliance requirements such as exhaustive risk assessments, quality assurance, and transparent documentation. For example, predictive AI models used in UC4 to anticipate patient deterioration require rigorous testing for bias and accuracy, detailed documentation for transparency, and continual risk assessments. Resource constraints and the complexity of maintaining ongoing algorithm validation processes make this compliance challenging yet essential for ensuring patient safety and regulatory approval.

General Data Protection Regulation (GDPR)

GDPR compliance is critical in UC4, mandating stringent measures for securing patient data through anonymization, pseudonymization, and explicit informed consent. In practical UC4 scenarios, such as real-time monitoring and predictive alerting, data must be processed

securely and compliantly, with explicit consent obtained continuously (medium for this is a combination of service use agreement with the ability to decline use of services from the UIs when required). Real-time compliance is resource-intensive, especially when managing large datasets and dynamic consent processes, highlighting the complexity and costs associated with robust GDPR adherence.

Cyber Resilience Act (CRA)

Compliance with CRA in UC4 involves robust cybersecurity measures for digital home care devices and platforms. A scenario might involve securing IoT devices used for home patient monitoring against cyber threats that could compromise patient safety. UC4 proactively implements regular vulnerability assessments, advanced cybersecurity protocols, and dedicated incident response teams. Yet rapidly evolving cybersecurity threats require ongoing vigilance and adaptation, straining available resources, and specialized expertise.

Network and Information Security Directive 2 (NIS2)

In UC4, NIS2 compliance mandates stringent cybersecurity standards and rapid incident reporting. For example, if a cyber incident compromises home care monitoring devices, rapid detection and reporting protocols must be in place to mitigate impacts. Implementing such robust cybersecurity risk management practices requires substantial investments in monitoring systems, cybersecurity training, and continuous protocol updates, representing a considerable operational challenge for UC4.

Medical Device Regulation (MDR)

UC4 aligns closely with MDR through rigorous certification processes, comprehensive quality management systems, and continuous clinical evaluations. For instance, digital monitoring devices classified under MDR must demonstrate consistent reliability and safety through extensive validation studies and quality assurance practices. MDR compliance processes are complex and resource-intensive, presenting challenges to innovation timelines, particularly within iterative and agile UC4 development contexts. Despite these challenges, strict adherence to MDR remains indispensable for patient safety, legal compliance, and credibility.

4.4.3 UC4 Special considerations

International and general special notes about UC4 in the context of ethicality and legality

Digital Divide and Accessibility
UC4 actively addresses the digital divide by ensuring equitable accessibility and usability of home care solutions. This involves tailored technology solutions, multilingual support, and designs that accommodate different literacy levels and physical capabilities. However, fully bridging this divide remains challenging due to uneven technological infrastructure across regions and resource limitations for extensive user training programs.

Ethical Use of Predictive Analytics

Predictive analytics within UC4 must be ethically managed to minimize patient anxiety related to predictive alerts or recommendations. UC4 incorporates clinician oversight, transparent patient communications, and robust educational support for social and

healthcare staff to mitigate potential ethical concerns to the patient-users who might necessarily not have the ability to perceive the ethical issues and/or enact on them. Nevertheless, maintaining patient trust in predictive analytics remains an ongoing challenge, particularly concerning false-positive alerts and over-reliance on automated recommendations.

Continuous Ethical and Regulatory Review

UC4 acknowledges the necessity of continuous ethical and regulatory reviews due to evolving technology and healthcare practices. Establishing robust interdisciplinary review processes within UC4 ensures sustained ethical alignment and adaptability in regulatory compliance, albeit resource-demanding and operationally complex.

Patient-Centered Design and Engagement

Patient engagement and feedback are central to UC4's ongoing design processes. Systems are iteratively improved based on direct patient experiences, ensuring alignment with real-world needs and preferences. Continuous engagement, while essential, requires sustained resources and deliberate efforts to maintain active patient involvement, e.g. weekly meetings including social and healthcare staff and the technology developers, development working groups including technology developers and representatives from several social and healthcare organizations, electronic feedback channels and meaningful integration of feedback.
By thoroughly addressing these ethical viewpoints, legislative mandates, and additional considerations, UC4 remains ethically robust, legally compliant, and operationally effective, enhancing overall healthcare quality and patient outcomes.

National, special considerations about UC4 in the context of ethicality and legality

UC4 operates under several key Finnish legislative frameworks that specifically address data protection, patient rights, and the secondary use of health and social data. These laws include:

- Act on the Secondary Use of Health and Social Data (Laki sosiaali- ja terveystietojen toissijaisesta käytöstä, 552/2019): This act governs how patient data can be used beyond primary care, crucial for UC4's analytics and AI-based prediction models. Compliance necessitates establishing secure, anonymized data environments, posing technical challenges related to data anonymization and governance protocols.
- Client Data Act (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, Asiakastietolaki, 27.8.2021/784): It mandates standards for electronic patient record handling, directly impacting UC4's interoperability solutions. Maintaining adherence is challenging due to legacy systems and varying levels of digital maturity across healthcare providers.
- Act on the Processing of Client Data in Social and Health Care (Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä, 703/2023): This legislation outlines robust standards for data handling within health and social care settings. It emphasizes strong governance, consent mechanisms, and secure data exchanges, elements central yet challenging for UC4's complex data integration and management processes.
- Social Welfare Client Documents Act (Sosiaalihuollon asiakasasiakirjalaki, Laki sosiaalihuollon asiakasasiakirjoista, 20.3.2015/254): Regulates documentation standards for social welfare clients, relevant to UC4's integrated care documentation practices, requiring consistent, compliant data recording methods.

- Act on the Status and Rights of Patients (Potilaslaki, Laki potilaan asemasta ja oikeuksista, 785/1992): Defines fundamental patient rights, mandating clear information provision and consent practices within UC4's patient-centered digital interactions.
- Act on the Status and Rights of Social Welfare Clients (Sosiaalihuollon asiakaslaki, Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista, 812/2000): Stipulates essential rights for social welfare clients, reinforcing UC4's need for transparent communication and respect for client autonomy in digital solutions.
- Social Welfare Act (Sosiaalihuoltolaki, 30.12.2014/1301): Governs the provision of social welfare services, necessitating UC4's adherence to service quality, equity, and access standards in digital care provision.

Compliance with these national frameworks presents operational and technical challenges related to system interoperability, data privacy measures, and maintaining patient autonomy and rights in digital care contexts. UC4 addresses these through ongoing investment in robust data governance strategies, cross-organizational collaboration and training (via the mentioned Knowledge Center) on the abovementioned topics (of legal and ethical backgrounds listed) for technology developers and social and healthcare staff.
By thoroughly addressing these ethical viewpoints, legislative mandates, and additional considerations, UC4 remains ethically robust, legally compliant, and operationally effective, enhancing overall healthcare quality and patient outcomes.

4.5 Use Case 5: AI-enabled management of clinical documentation

Use case 5 explores the deployment of an AI (Artificial Intelligence) system that assists clinicians in managing clinical documentation. This may include automatic transcription of doctor-patient interactions, structuring unstructured notes into standard clinical formats, or summarizing large sets of clinical data to support diagnostics and treatment planning. The system does not make medical decisions autonomously but facilitates documentation processes, and integration into Electronic Health Record (EHR) systems.

4.5.1 UC5 Ethical considerations

The ethical principles outlined in Chapter 2, such as transparency, human oversight, fairness, and respect for fundamental rights remain highly relevant for AI-enabled clinical documentation but must be interpreted in light of its indirect yet foundational role in patient care. This use case presents unique challenges and obligations, particularly when integrated with EHR systems or deployed in-house within health institutions.

Transparency and explainability

While Chapter 2 emphasizes full transparency for systems influencing clinical decisions, documentation AI must ensure explainability in how text is generated or transformed, including visibility into speech-to-text processing, autocomplete mechanisms, and data provenance. Errors in documentation, while not decision-making in themselves, may mislead subsequent clinical judgment. According to the AI Act Article 52, clinicians must be clearly informed about AI assistance, especially when suggestions are context sensitive.

Human oversight and accountability (MDCG 2025-6 update[1])

Chapter 2 calls for human-in-the-loop control for high-risk systems. For documentation AI, this implies that clinicians must retain editorial control, with audit trails and version history to support corrections and traceability. Notably, MDCG (Medical Device Coordination Group) affirms that even in-house tools, though exempt from notified body review, are not exempt from oversight or professional accountability obligations, highlighting the enduring ethical duty to validate outputs.

Bias and fairness in representation

Documentation tools risk introducing linguistic or clinical bias, for example by favoring certain phrasing styles or neglecting dialects, non-native speaker input, or minority health narratives. Unlike diagnostic AI, these biases may be more insidious as they influence the record itself rather than an immediate decision. Mitigation requires representative training datasets, language diversity testing, and bias audits for post-deployment.

Patient autonomy, consent, and surveillance concerns

While Chapter 2 emphasizes human dignity and autonomy, AI-enabled clinical documentation introduces additional ethical challenges, particularly when the system captures or processes of spoken communication. To address these concerns, explicit informed consent is obtained in a structured, multi-step process. Participants (nursing

students in simulated learning situations) receive a written information sheet and a GDPR-compliant privacy notice that clearly describe the purpose of voice recording, its use for AI model development, the storage environment, and the fact that voice data cannot be anonymized or later removed once integrated into model training datasets. Consent is provided in writing, and all individuals present in a recorded session must consent for the recording to proceed.
To ensure understanding of AI's role, the information materials specify how the data will support AI model training, what technical safeguards are applied, what risks are associated with voice data, and the boundaries of participant rights. Only designated personnel may access the data, and usage outside the project requires an ethical review and a dedicated data-use agreement. This process helps mitigate surveillance concerns by ensuring that participation is voluntary, informed, and limited to pedagogical simulations, not real patient interactions, while maintaining transparency about the involvement of AI technologies.

Ethical expectations despite regulatory exemptions (MDCG 2025-6 update[1])

The recent guidance makes it clear that in-house clinical documentation tools, even when exempt from full MDR notified body assessment, must still uphold ethical and safety obligations, especially within institutional governance frameworks. This underscores that regulatory relief does not equate ethical leniency.

Practical ethical handling in use case 5

In Use Case 5, ethical considerations were addressed not only through the identification of ethical principles but through concrete procedural steps that guided the development and evaluation of the AI-supported clinical documentation system. Because the work involved the collection of audio data in simulated clinical interactions, TUAS implemented a structured ethical governance process before any data collection began.

First, the study design and data collection procedures were reviewed and approved by TUAS's ethics committee, ensuring that the project met established standards for research involving human participants. In parallel, TUAS conducted a Data Protection Impact Assessment (DPIA) to analyse the privacy risks associated with processing voice recordings, which are non-anonymisable personal data. The DPIA informed mitigation measures including restricted access, secure storage, strict role assignment, and purpose limitation.

Ethical reflections were further operationalised through ongoing internal discussions among developers (Mediconsult) and TUAS domain experts. These discussions focused on anticipating potential impacts on participants, evaluating the proportionality of data use, and agreement on acceptable risk boundaries. As a result, several practical decisions were made: limiting data collection to pedagogical simulations (no real patients), excluding identifiable metadata, and ensuring that recordings were never used for student assessment or performance monitoring.

Informed consent was central to the process. All participants received clear written information explaining what data would be collected, how it would be processed, stored, and reused, and what limitations exist due to the impossibility of fully anonymising voice data. Recording proceeded only when every individual in the simulation provided written consent, thereby safeguarding autonomy and preventing participation pressure in a learning environment.

For collaboration with project partners and technology providers, additional ethical and privacy safeguards were formalised contractually. Any organisation receiving temporary access to the audio material was required to provide a detailed usage plan demonstrating how they would ensure that AI models trained on the data would not contain sensitive or identifiable information, nor allow reconstruction of the original recordings. All parties committed to complying with the GDPR, the Finnish Data Protection Act, and the EU AI Act. Each organisation designated a responsible person for the handling and deletion of data at the end of the permitted period, ensuring accountability and traceability.

Together, these procedures show that ethical considerations in Use Case 5 were not merely theoretical principles but were embedded into practical actions, institutional oversight, privacy risk assessment, and transparent consent processes. This approach reflects the "soft regulation" dimension as ethics was implemented through anticipation of human behaviour, protection of participant wellbeing, and attention to the societal acceptability and trustworthiness of the resulting AI technology.

4.5.2 UC5 Legislative considerations

AI-enabled clinical documentation systems generally fall under the high-risk AI category as defined in the AI Act, particularly when they impact health-related functions. Unlike many high-risk AI systems covered in Chapter 3 (i.e., recruitment, public administration), this use case is further complicated by dual classification under medical device regulations (MDR) and EHR legislation (EHDS), creating a layered regulatory environment.

Dual regulatory classification: AI Act + MDR

As per the AI Act, AI systems used in healthcare are typically high-risk, requiring compliance with Annex III and Title III obligations, including risk management, data governance, human oversight, and technical documentation.
However, if the AI documentation system meets the definition of Medical Device Software (MDSW), in example if it supports or influences diagnosis/treatment decisions, it also falls under the MDR, most often Class IIa or higher per Rule 11, triggering conformity assessment procedures.
Compared to Chapter 3, UC5 is more complex due to MDR co-applicability and additional post-market surveillance requirements.

In-house tool exemption clarified (MDCG 2025-6 update[1])

The recently published MDCG 2025-6 clarifies that AI-based clinical documentation tools developed and used exclusively in-house by healthcare institutions may be exempt from full notified body assessment, even if they fall under Class IIa (MDR).
This diverges from Chapter 3, where high-risk classification invariably leads to regulatory assessment. However, the exemption is conditional, and such tools must still meet general safety and performance requirements, and institutions remain legally responsible for clinical validation and risk control.
This creates a differentiated compliance path for public health providers using in-house AI compared to commercial vendors.

[1] https://health.ec.europa.eu/latest-updates/mdcg-2025-6-faq-interplay-between-medical-devices-regulation-vitro-diagnostic-medical-devices-2025-06-19_en.

Online platform distribution – new rules from MDCG 2025-4[2]

If the AI-enabled documentation tool is distributed via online platforms, including mobile app stores or cloud-based services, it must now comply with MDCG 2025-4.
This introduces obligations overlapping with the Digital Services Act (DSA), such as traceability, safe withdrawal mechanisms, and provider transparency, requirements not addressed in Chapter 3 for other sectors.
For hospital systems deploying third-party documentation tools, these new platform-specific rules require updated procurement and IT governance protocols.

Revised software classification rules (MDCG 2019-11 rev1[3])

The updated MDCG 2019-11 (2025) provides expanded examples of how software qualifies as MDSW and further clarifies classification under Rule 11.

It now explicitly includes AI-powered documentation systems integrated with EHRs and adds clarity on the difference between informational vs. therapeutic impact, a legal distinction essential for risk classification. Compared to Chapter 3, where risk stratification is mostly defined by AI function alone, UC5 is further influenced by the context of clinical use.

EHDS and data use implications

When AI systems process documentation data for secondary use (i.e., performance retraining, NLP model improvement), the European Health Data Space (EHDS) regulation applies. EHDS imposes conditions on data interoperability, pseudonymization, and access rights for patients and providers by introducing additional legal complexity compared to non-health data AI in Chapter 3.

4.5.3 UC5 Special considerations

The use of AI-enabled EHR systems is influenced by multiple EU-wide and national developments that extend beyond the ethical and legislative frameworks described in Chapters 2 and 3. The following considerations highlight evolving dynamics.

National implementations of EHDS and AI Act

Several Member States (i.e., Finland, Denmark, Germany) are leading national-level preparations for EHDS integration, particularly in structuring Health Data Access Bodies (HDABs) and defining technical specifications for secure AI training environments.
For developers or health institutions involved in cross-border AI deployment, alignment with national data interoperability protocols is critical, as discrepancies in EHDS implementation may affect data access rights, patient consent, and data portability.
And chapter 3 does not account for these national discrepancies in implementation, which are especially important for AI in healthcare due to sensitive personal data categories.

Interaction with hospital procurement policies and internal governance

[2] https://health.ec.europa.eu/latest-updates/mdcg-2025-4-guidance-safe-making-available-medical-device-software-mdsw-apps-online-platforms-june-2025-06-16_en.
[3] https://health.ec.europa.eu/latest-updates/update-mdcg-2019-11-rev1-qualification-and-classification-software-regulation-eu-2017745-and-2025-06-17_en.

Public hospitals and regional health authorities increasingly require internal validation and ethics oversight even for in-house AI tools that are exempt from MDR Notified Body review per MDCG 2025-6. Many institutions follow local ethical AI frameworks, such as those developed by the Finnish Ministry of Social Affairs and Health, which often impose pre-deployment evaluation boards or transparency assessments. These institution-specific frameworks are not captured in Chapters 2 or 3 but play a significant role in approvals and trust at the local level.

Real-world performance monitoring requirements

National health systems (i.e., NHS England, Kela Finland) are beginning to require real-world performance dashboards or audit trails for AI-enabled EHR tools, sometimes as a condition of funding or integration. This mirrors MDR post-market surveillance but is applied even to in-house tools not subject to formal CE-marking, highlighting a trend toward decentralized assurance mechanisms.
Chapter 3 outlines AI provider obligations for performance but does not address health system-driven oversight, which is increasingly influential.

Impacts of integration with national EHR systems

AI-enabled EHR tools that input into or extract from national health systems (i.e., Kanta in Finland) must comply with system-specific integration rules. These may include semantic interoperability standards (i.e., HL7 FHIR), data retention laws, and limitations on cross-border data export.
Such technical-legal constraints are outside the AI Act and MDR but can significantly affect deployment feasibility and updating cycles.

Cybersecurity as an independent governance layer

While EU regulations such as MDR and the AI Act address robustness and safety, cybersecurity obligations remain fragmented. AI-enabled documentation tools face heightened risks of data breaches, ransomware, and adversarial attacks, which can undermine both privacy and clinical reliability.

National agencies like NCSC-FI (National Cyber Security Centre Finland) and ENISA (EU agency dedicated to enhancing cybersecurity in Europe) guidance and sector-specific standards (i.e., ISO/IEC 81001-5-1 for health software) increasingly impose additional safeguards not covered in Chapters 2 or 3. This creates a parallel governance layer where compliance must be demonstrated through secure coding practices, penetration testing, and continuous monitoring.

Risk-based approach as a continuous requirement

The MDR embeds risk-based thinking in product classification and conformity assessment, and the AI Act adopts a similar logic by assigning obligations according to risk tier. However, both frameworks often treat risk as a static compliance step rather than a continuous process.

For clinical documentation AI, risk must be reassessed across the lifecycle, covering clinical harms (i.e., misdocumentation), operational impacts (i.e., workflow disruption), and systemic issues (i.e., bias propagation). This extends beyond the Chapter 3 perspective by emphasizing dynamic, recurring risk management linked to real-world use and evolving clinical contexts.

4.6 Use Case 6: Smart orchestration of services for optimized customer and care pathways

This use case addresses the coordination and sequencing of healthcare, social care, and related services through a smart orchestration system. By integrating data and process flows from multiple providers, the system aims to deliver a coherent pathway that meets individual needs of customers and health and social care professionals while improving efficiency and resource allocation. Ethical and legal considerations for UC6 arise from its cross sector nature, combining data, workflows, and decision-making- responsibilities from domains governed by distinct regulations and professional norms. The following subsections examine how the ethical principles, legislative requirements, and special considerations apply to UC6, highlighting both commonalities with other PROFIT use cases and challenges unique to this orchestration context.

4.6.1 UC6 Ethical considerations

The orchestration of customer and care pathways presents distinctive ethical dimensions compared to other use cases described in Chapter 2. While many of the Trustworthy AI principles apply universally, UC6's context of integrating health, social, and potentially community services introduces complex cross sectoral considerations.

Human agency and oversight in UC6 must account for the fact that decision-making is distributed across multiple professional domains. The system should augment coordination without diminishing the autonomy of any stakeholder group, ensuring that final service pathway decisions remain with qualified human actors in both healthcare and social care sectors. Maintaining clear accountability at each decision point becomes more challenging when orchestration spans organisational boundaries.

Privacy and data governance gain additional complexity in UC6 because personal information may originate from different sectors, governed by distinct rules and expectations. Ethical alignment requires the system to respect the highest applicable privacy standards across all data types, while ensuring that individuals retain clarity and control over how their information is shared for pathway orchestration purposes.

Transparency and explainability in UC6 go beyond informing users that AI or automation is involved. Professionals and service recipients should be able to understand the rationale for orchestration outcomes — for example, why certain services are sequenced or prioritised — even when this logic involves multifactor inputs from multiple systems. The conceptual challenge lies in conveying these explanations in ways accessible to diverse stakeholders with different technical, clinical, and social backgrounds.

Fairness and non-discrimination are critical when orchestrating pathways that influence access to services. The system must avoid embedding biases that could result in unequal allocation of services, either through historical patterns in source data or through prioritisation logic that inadvertently favours certain groups. Compared to the general ethical principles, UC6 has heightened exposure to fairness risks because it balances resources across various service categories.

Accountability must be clearly defined among participating stakeholders. Ethical governance in UC6 should ensure that, even when multiple organisations contribute data or execute parts of the pathway, there is traceability of decisions and a recognised locus of responsibility for each segment of orchestration.

These considerations extend the general principles outlined in Chapter 2 by applying them to a multidomain, multiactor environment. Ethical soundness in UC6 depends not only on compliance with overarching Trustworthy AI guidelines but also on the ability to reconcile different sectoral norms and expectations into a coherent, transparent, and fair orchestration process.

4.6.2 UC6 Legislative considerations

The legislative landscape for UC6 is shaped by its role as an orchestrator spanning healthcare, social care, and potentially community services. While Chapter 3 outlines overarching obligations under EU laws such as the GDPR, EHDS Regulation, EU AI Act, and other sector specific instruments, UC6's cross domain nature means these frameworks often overlap and must be applied in combination.

Under the General Data Protection Regulation (GDPR), UC6 processes special category data from multiple sources, including health records and social service files. Legislative alignment requires a lawful basis for each processing purpose, strict data minimisation, and safeguards appropriate to the most sensitive data in the orchestration flow. Compared to single domain use cases in Chapter 3, UC6 faces higher governance complexity because integrated pathways may involve differing consent regimes or retention requirements across sectors.

The European Health Data Space (EHDS) Regulation is particularly relevant where UC6 facilitates secondary use of health data for service planning or quality improvement. Harmonising EHDS rules with social care data frameworks present a distinctive legal challenge, as EHDS is primarily healthfocused. Secure processing environments and compliance with pseudonymisation and reidentification prohibitions are required for any reuse of patient health data within orchestration logic.

If UC6 employs AI driven prioritisation or decision support features, the EU AI Act may classify the system as a high-risk AI application. In this case, obligations such as documented risk management, data governance measures, transparency provisions, and human oversight mechanisms must be met. Compared to other high-risk systems described in Chapter 3, UC6's AI oversight measures must accommodate multiple stakeholder types, potentially with different operational protocols.

Compliance with Data Governance Act (DGA) provisions may also be triggered if UC6 participates in, or contributes to, shared data spaces or supports voluntary data donation for pathway optimisation. In such cases, UC6 must ensure neutrality in data intermediation and align with DGA transparency and security expectations.

Cybersecurity obligations outlined in NIS2 and, where applicable, the Cyber Resilience Act (CRA), apply to the orchestrator's infrastructure, especially if it forms part of essential digital services in healthcare or social welfare. UC6 may require governance measures that go beyond those in Chapter 3 because it could be designated as part of critical infrastructure due to its role in coordinating essential services.

The Medical Device Regulation (MDR) may apply if UC6's core functions influence clinical decisions or patient care pathways in a way that meets the definition of medical device software. In such cases, conformity assessment, CE marking, and quality management procedures become relevant. However, orchestration functions that primarily handle administrative sequencing without impacting direct clinical decision-making may be outside MDR scope.

In summary, UC6's legislative considerations require careful mapping of sector specific obligations and resolution of overlaps between legal regimes. Legislative compliance must be scoped to the most stringent applicable requirements, ensuring that the orchestration environment operates lawfully across all participating domains.

4.6.3 UC6 Special considerations

Beyond the common ethical and legislative frameworks described in Chapters 2 and 3, UC6 faces distinctive operational and governance conditions arising from its cross-sector scope and integration role. These special considerations include:

National frameworks and sectorspecific regulations

UC6 must account for national laws governing both health and social care data, which may impose specific consent procedures, interoperability standards, or documentation requirements. For example, legislation on the secondary use of health data or on social welfare client records can directly shape how orchestration logic is implemented and what information can be shared between systems.

Cross-organisational interoperability and governance

The orchestrator's effectiveness relies on cooperation among diverse organisations, each with its own policies, IT maturity level, and risk tolerance. Achieving consistent pathway management may require formal agreements, joint governance bodies, and harmonised operational protocols that go beyond statutory requirements.

Stakeholder diversity and expectation management

UC6 serves multiple user groups — healthcare providers, social workers, service managers, and citizens — each with varying expectations for responsiveness, service scope, and privacy. Special attention must be given to aligning these expectations, especially when orchestration outcomes involve tradeoffs between resource constraints and service priorities.

Non-health data integration

In addition to clinical and social care information, UC6 may draw on administrative or contextual data (e.g., housing services, community programms, transportation options). These datasets may fall under separate regulatory regimes or lack the formal protections common in health law, requiring tailored governance measures to ensure ethical treatment and quality assurance.

Local policy alignment

Municipal or regional authorities may have service coordination policies or care pathway models that influence how orchestration is configured. Compliance with these policies, while

not mandated at the EU or national legislative level, is essential for operational acceptance and long-term sustainability within local service ecosystems.
In sum, UC6's special considerations highlight the need for adaptable governance mechanisms capable of reconciling different legal traditions, organisational cultures, and service models. These elements, while operating outside the explicit scope of Chapters 2 and 3, are critical to delivering ethically robust and legally sound orchestration of customer and care pathways.

5 Ethics and legislation in nursing education

Since many users of the technology developed in the project are nurses, it is worth examining how ethical principles and laws governing nursing are taken into account during nursing education. This chapter provides an overview of the ethical and legal foundations of nursing practice in Finland, with a particular focus on the education and training of nurses at Turku University of Applied Sciences. The chapter outlines the key regulations and ethical principles that guide professional conduct, patient care, and data protection, while highlighting how these elements are integrated into the nursing curriculum to ensure competence, safety, and accountability in healthcare settings. This is not an EU-level or even a Finnish-wide review, but rather a good example of high-quality nursing education with strong foundation in ethical and legal principles.

Ethical and legal aspects of nursing

In Finland, the work of a registered nurse is governed by a robust ethical framework and comprehensive legal regulations that safeguard patient safety, uphold high standards of care, and protect human dignity and rights. The ethical principles for nurses are defined by the Finnish Nurses Association and are consistent with the International Council of Nurses (ICN) Code of Ethics.

From a legal perspective, several key laws and regulations shape nursing practice:

- The Act on Health Care Professionals outlines the rights and responsibilities of healthcare professionals, including qualification, registration, and professional conduct requirements.
- The Patient Act ensures patients' rights to quality care and treatment, emphasizes informed consent and the right to refuse treatment, and regulates access to medical records and confidentiality.
- Data protection and privacy laws, including the General Data Protection Regulation (GDPR), require nurses to handle personal data and patient records in accordance with EU and Finnish legislation.
- The Decree on the Language Proficiency of Healthcare Professionals mandates sufficient language skills for safe and effective communication in patient care.
- The Social Welfare and Health Care Client Data Act governs the processing, recording, and sharing of patient data within digital healthcare systems.
- The Occupational Safety and Health Act defines nurses' rights and responsibilities in maintaining a safe working environment and ensuring both patient and occupational safety.
- EU Directives 2005/36/EC and 2013/55/EU regulate the recognition of professional qualifications and establish standards for nursing education and competence across EU countries.
- Pharmaceutical legislation requires nurses to comply with laws regulating pharmacotherapy, prescription practices, and medication safety. In Finland, the safe and effective administration of medication is a legally regulated responsibility within social and healthcare services. To ensure compliance with national legislation and uphold high standards of patient safety, every healthcare unit is required to implement a comprehensive medication plan. This plan serves as a strategic framework for guiding medication practices and ensuring that pharmacotherapy is carried out professionally and responsibly. In addition to internal planning, nurses must comply with both national and EU-level pharmaceutical legislation. This includes requirements such as the Medication Passport and LOVe (Safe Pharmacotherapy) training, which are designed to

verify and maintain nurses' competence in medication management. These tools support safe pharmacotherapy by ensuring that nurses have up-to-date knowledge and skills in medication administration, calculation, and patient safety.

Overview of the nursing curriculum at Turku University of Applied Sciences

Finland has approximately 73 600 nurses in the workforce. The Bachelor of Nursing degree is offered at universities of applied sciences across Finland. Applicants must hold a secondary education qualification, such as a matriculation examination or a vocational qualification. Each year, approximately 4 500 nurses graduate from these institutions with qualifications in general nursing. Turku University of Applied Sciences (Turku UAS) educates approximately 300 nurses annually.

The Bachelor of Nursing program at Turku University of Applied Sciences provides students with a comprehensive education that prepares them for professional nursing roles in various healthcare environments. The degree consists of 210 ECTS credits (European Credit Transfer and Accumulation System) over 3,5 years, including extensive practical training in accordance with EU requirements. Graduates are eligible to apply for professional practice rights from Valvira, enabling them to work in hospitals, health centers, outpatient clinics, private practices, and other healthcare or social care institutions.

A distinctive feature of the curriculum is its strong foundation in ethical and legal principles. The program is designed to ensure that students understand and adhere to the ethical standards set by the Finnish Nurses Association and the International Council of Nurses (ICN) Code of Ethics. These principles guide nurses in promoting patient safety, dignity, and high-quality care. Legal aspects are deeply integrated into the curriculum, reflecting both Finnish and European regulations. Students learn about the laws governing healthcare professionals, patient rights, data protection, language proficiency, and occupational safety. The curriculum also covers EU directives that regulate professional qualifications and set standards for nursing education and competence across member states. Throughout their studies, students develop the ability to assess, plan, and implement nursing care using current scientific knowledge. The curriculum emphasizes interdisciplinary teamwork, evidence-based practice, and the promotion of healthy lifestyles. Students are trained to respond effectively in emergencies, support patients and families, and evaluate the quality of care. Communication skills and continuous professional development are also key components.

Ethical and legal themes are present in several courses and are also deeply embedded in supervised clinical training, which amounts to 90 ECTS credits throughout the curriculum. This clinical training provides students with extensive hands-on experience in real healthcare environments. It is essential for developing practical nursing competencies, applying theoretical knowledge in real-world settings, and fostering professional growth. The curriculum ensures that graduates are equipped to handle complex situations involving patient rights, safe care practices, and decision-making in clinical settings. The curriculum also supports lifelong learning, sustainable development, and the ability to adapt to new challenges in a digitalized healthcare sector.

6 Conclusion

This document analyzes the legal and ethical requirements for the PROFIT project, focusing on European regulations and ethical frameworks to ensure patient safety and data protection.

Chapter 2 provided the ethical foundations and guiding principles for trustworthy AI and also described the research-ethics governance process that underpins the project while Chapter 3 discussed the most important legislation from the project perspective.

A review of the six use cases presented in Chapter 4 highlights several consistent themes and shared priorities. Each use case is primarily guided by the principles of fairness, transparency, accountability, and safety, implemented through strict adherence to the General Data Protection Regulation (GDPR), the EU Artificial Intelligence Act (AI Act), the Medical Device Regulation (MDR), and the European Commission's Ethics Guidelines for Trustworthy AI. Emphasis is placed on data protection by design, robust data governance, and risk minimization concerning sensitive health data. Standard practices include conducting Data Protection Impact Assessments (DPIAs) and implementing accurate access controls. AI systems are designed to support, not replace, human decisions, with embedded human oversight mechanisms such as the ability to override AI recommendations. Continuous validation and monitoring protect reliability and safety, especially in clinical decision-making. The innovations introduced by the PROFIT project are intended to enhance patient outcomes, staff experiences, and operational efficiency, while also considering the broader societal and environmental impacts of digital healthcare.

Despite the notable differences between the project use cases, they all share the same overarching requirements, limitations, and implementation challenges associated with introducing new technology in healthcare services. Compliance requires an integrated approach combining regulatory adherence, strong cybersecurity, ethical decision-making, staff training, and continuous monitoring. A transparent and secure data environment strengthens trust, protects patient rights, and supports clinical excellence.

Chapter 5 addressed the integration of ethical and legal standards into nursing education, ensuring that future professionals are equipped to uphold these requirements in practice.

While this document provides a robust framework for legal and ethical compliance, several limitations must be acknowledged. The regulatory landscape, especially concerning AI and health data, is rapidly evolving, which means that some sections of this document may become outdated as new laws and guidelines are introduced. The focus here is on EU-level regulations, and national laws are addressed only when directly relevant to specific use cases. As a result, local implementation may require further analysis. Additionally, differences in digital maturity and organizational practices across healthcare providers can make it challenging to apply these requirements uniformly.

To maintain compliance and ethical standards, regular updates to legal and ethical assessments are essential to keep pace with changes in legislation and technology. It is important to maintain the active involvement of clinicians, patients, and stakeholders throughout the design, deployment, and evaluation of AI systems, as this helps to identify new risks and usability challenges. Continued investment in interoperable systems and adherence to international standards will foster secure data exchange and scalability. Providing training and support for end-users is crucial for the effective adoption of new technologies. The internal ethics committees and review processes will reinforce

accountability and public trust. By integrating these principles and practices into the PROFIT project, the consortium not only fulfills its legal and ethical responsibilities but also lays a strong foundation for trust and sustainability in the future deployment of AI in healthcare.