Project Title	ENsuring Secure and Safe CMD Design with Zero TRUST Principles		
Project Acronym	ENTRUST		
Grant Agreement No	101095634	Type of Action	Research and Innovation Action
Call / Topic	HORIZON-HLTH-2022-IND-13-01		

D1.3 Legal and Ethical Issues and Guidelines

Work Package	WP1 Project Management		
Lead Beneficiary	Future Needs Management Consulting Ltd.		
Contributing Beneficiaries	All beneficiaries		
Due Date	31.12.2024	Actual Date of Submission	27.12.2024
Version	0.9		
Authors	Athanasios Arvanitidis, Anna Palaiologk, Panos Chatzimathios (FN), Adrian Quesada Rodriguez, Renáta Radocz, Sébastien Ziegler (MI), Angelina Broukou, Maria Karampela (UNIS LUX), Symeon Tsintzos (QUBI), Dimitris Karras (UBI)		
Abstract	Deliverable D1.3, Legal and Ethical Issues and Guidelines outlines the legal framework and ethics policy adopted by the ENTRUST project to ensure compliance with EU legislation, ethical assurance, and inclusivity. It integrates findings from workshops, surveys, and earlier deliverables to address key concerns in data protection, cybersecurity, and trust in Connected Medical Devices (CMDs). The analysis emphasises ethical issues related to evidence measures and trustworthiness in CMDs, ensuring alignment with current medical standards. By embedding ethical principles and regulatory alignment, ENTRUST provides a robust framework for secure, trustworthy CMDs that meet societal needs.		
Keywords	Connected Medical Devices, Ethical Guidelines, Legal Compliance, Trustworthiness, Gender Balance		

The project ENTRUST has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101095634

Versioning and contribution history

Version	Date	Author	Notes
0.1	01.10.2024	Athanasios Arvanitidis (FN)	Creation of ToC
0.2	01.10.2024	Maria Karampela (UNIS LUX)	Refinements on the ToC
0.3	02.12.2024	Athanasios Arvanitidis (FN)	Initial version of document
0.4	09.12.2024	Athanasios Arvanitidis (FN)	Inputs
0.5	11.12.2024	Adrian Quesada Rodriguez, Renáta Radócz. Sébastien Ziegler (MI)	Added inputs on legal/certification perspectives
0.6	13.12.2024	Angelina Broukou, Maria Karampela (UNIS LUX)	Overall review of the status and inputs
0.7	23.12.2024	Athanasios Arvanitidis, Anna Palaiologk, Panos Chatzimathios (FN)	Updates
0.8	23.12.2024	Anna Palaiologk (FN)	Overall review of the status
0.9	23.12.2024	Athanasios Arvanitidis (FN)	Draft for final review and submission
1.0	27.12.2024	Angelina Broukou (UNIS LUX)	Final review & submission

Funded by the Horizon Framework Programme of the European Union

Disclaimer

COPYRIGHT NOTICE

Project co-funded by the European Commission in the Horizon Programme		
Nature of the deliverable:	*R	
Dissemination Level		
PU	Public, fully open	X
SEN	Sensitive, confidential to ENTRUST project and Commission Services	

* R: Document, report (excluding the periodic and final reports)
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
OTHER: Software, technical diagram, etc.
DMP: Data Management Plan

Funded by the Horizon Framework Programme of the European Union

Glossary of terms and abbreviations used

Term	Description
AIMDD	Active Implantable Medical Devices Directive
AI	Artificial Intelligence
AI HLEG	High-Level Expert Group on Artificial Intelligence
CIOMS	Council for International Organizations of Medical Sciences
CMD	Connected Medical Device
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRTs	Security Incident Response Teams
DGA	Data Governance Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECCG	EU Cybersecurity Certification Group
EDIB	European Data Innovation Board
EHDS	European Health Data Space
EHR	Electronic Health Record
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCC	European Common Criteria-based Certification Scheme
GA	Grant Agreement
GDPR	General Data Protection Regulation
GSPRs	General Safety and Performance Requirements
ICT	Information and Communication Technology
IoT	Internet of Things
ISO	International Organization for Standardisation
IVDR	In Vitro Diagnostic Medical Devices Regulation
MDCG	Medical Device Coordination Group
MDD	Medical Devices Directive
MDR	Medical Device Regulation
NIS2	Network and Information Security Directive 2
PMS	Post-Market Surveillance
RED	Radio Equipment Directive
SaMD	Software as a Medical Device
SMEs	Small and Medium-Sized Enterprises
UDI	Unique Device Identifier
WHO	World Health Organisation

Funded by the Horizon Framework Programme of the European Union

Table of Contents

Funded by the Horizon Framework Programme of the European Union

Funded by the Horizon Framework Programme of the European Union

Funded by the Horizon Framework Programme of the European Union

List of Figures

Funded by the Horizon Framework Programme of the European Union

List of Tables

Funded by the Horizon Framework Programme of the European Union

Executive Summary

Deliverable D1.3, **Legal and Ethical Issues and Guidelines**, defines the legal framework and ethics policy adopted by the ENTRUST project. Its primary objective is to ensure ethical assurance, gender equality, and full compliance with national and EU legislation throughout the project's lifecycle. By addressing critical legal and ethical considerations, ENTRUST ensures that Connected Medical Devices (CMDs) are secure, trustworthy, and aligned with societal needs. The deliverable builds on insights from earlier project activities, including the **Data Management Plans (D1.2 and D1.4)** and the **ENTRUST Reference Architecture deliverables (D2.1 and D2.2)**. A dedicated **workshop** and two **surveys**—one targeting technology users and another focusing on citizens—were conducted to gather feedback on ethical, legal, and societal aspects of CMDs. These activities revealed actionable insights into public and professional attitudes, emphasising the importance of robust cybersecurity, transparent communication, and ethical compliance. The deliverable proposes recommendations, including revising **MDCG 2019–16** to include harmonised security requirements and runtime evidence, promoting open access, and fostering stakeholder engagement to enhance inclusivity. ENTRUST also advocates standardising IT security for CMDs to address gaps in trustworthiness. By integrating ethical principles, complying with EU regulations, and engaging stakeholders, ENTRUST sets a foundation for developing CMDs that prioritise trustworthiness, security, and societal acceptance. The findings and recommendations in this deliverable guide ENTRUST's ongoing efforts to advance CMD development responsibly and inclusively.

Funded by the Horizon Framework Programme of the European Union

1 Introduction

1.1 Purpose of the document

Deliverable *D1.3, Legal and Ethical Issues and Guidelines*, aims to define and present the legal framework and ethics policy adopted by the ENTRUST project. The primary objective is to ensure ethical assurance, gender equality, and full compliance with national and European Union (EU) legislation throughout the project's lifecycle. To support these goals and upscale the project's outcomes, a dedicated workshop on the ethical and legal dimensions of CMDs was conducted within the consortium. This workshop facilitated mapping of current frameworks and dimensions. Additionally, two surveys were carried out: (i) Survey for Technology Users and End Users: To gather insights regarding ethical and legal considerations in CMDs. (ii) General Public Survey: To explore perspectives on transparency, security, and trust in CMDs. Parts of the ethical considerations were previously outlined in the [1] D1.4 "*Data Management Plan*" [1]. Similarly, aspects of the legal framework were integrated into the deliverables detailing the initial and final release of the ENTRUST Reference Architecture (D2.1, D2.2) [2], [3]. These documents collectively establish the overarching approach, mechanisms, and procedures for monitoring legal and ethical compliance, as identified in the Grant Agreement (GA). The final, consolidated, and revised version of these elements is delivered in M24, capturing and validating the project's legal and ethical requirements at a more mature stage. The ethics principles have been embedded across all phases of project implementation, particularly in data management and processing activities. Ethical considerations, data protection legislation, and related guidelines have been applied during all procedures. Furthermore, the ethics framework was integral to stakeholder workshops and expert interviews, ensuring compliance and inclusivity. Additionally, an ethical and legal framework was critical in the earlier stages of the project, especially during the definition of various components and elements of the ENTRUST system architecture (WP2, WP3, WP4, WP5 & WP6). This ensured that foundational aspects of the project adhered to ethical and legal standards from the outset.

1.2 Scope and Objective

The scope of this manual is to establish a comprehensive Legal and Ethics Guide for all researchers involved in the ENTRUST project. As a living document, it evolves to reflect the continuous, multi-dimensional, and layered flow of information within the project. It is essential to define the overarching legal and ethical principles that govern all ENTRUST activities, including pilots and other project-specific activities. This ensures that the ethical and legal dimensions of CMDs and related sectors are thoroughly addressed. To support this effort, insights gathered

Funded by the Horizon Framework Programme of the European Union

from end-users and the general public are incorporated, offering diverse perspectives that enrich and guide the research process.

A dynamic approach to applying legal and ethical principles across various project activities is essential. This document outlines principles and guidelines tailored to different user clusters, addressing their specific needs and responsibilities, including:

- WP2: Requirements Analysis, Gap Analysis, and Reference Trust Architecture.
- WP3: Trust Modelling, Risk Assessment, and Security-by-Design Toolbox.
- WP5: Secure Lifecycle Management and Dynamic Trust Assessment, including the Integration and Validation of the Trust Management Framework through Use Cases.
- WP7: Stakeholder Engagement and Feedback Mechanisms.
- Consortium Members: Particularly those involved in development, data management, piloting, testing, treatment, analysis, reporting, and communication activities.
- Engagement and Recruitment Teams: To ensure ethical standards are upheld during stakeholder engagement and recruitment processes.
- Ethics Committee: To monitor and oversee the application of ethical guidelines.

This document is also designed to serve as a Legal & Ethics Guide for similar service-oriented projects in the fields of CMDs and Trust Management, ensuring transferability and wider applicability of the ENTRUST project's ethical and legal framework.

1.3 Structure of the document

This deliverable is structured into five main chapters, systematically covering the objectives, methodology, and findings of the ENTRUST project regarding the legal, ethical, and societal dimensions of cybersecurity in CMDs.

In **Chapter 1** "**Introduction**", the introduction outlines the purpose, scope, and objectives of this document. It sets the foundation for understanding how the ENTRUST project integrates legal, ethical, and technical perspectives to develop a trustworthy framework for CMDs.

Chapter 2 delves into **Legal and Ethical Considerations**, highlighting critical regulations, frameworks, and ethical principles that govern CMDs. It examines key legislation such as the GDPR, Cybersecurity Act, MDR, and AI Act, while exploring principles like Trustworthy AI and ethical frameworks for clinical research. This chapter provides a comprehensive overview of the regulatory landscape relevant to CMDs.

Chapter 3 addresses the **Societal Dimensions** of CMDs, focusing on public and professional attitudes toward cybersecurity, trust, and ethical compliance. It includes results from workshops and questionnaires conducted with end-users, clinicians, and citizens. Furthermore, the chapter

Funded by the Horizon Framework Programme of the European Union

discusses the challenges and strategies for designing CMDs that meet societal readiness, emphasising frameworks such as system engineering thinking and the integration of end-user feedback.

Chapter 4 is titled **ENTRUST Contributions to Legal, Ethical, and Regulatory Frameworks**. It discusses ENTRUST's role in regulatory compliance, alignment with legal and ethical requirements, and recommendations for improving current guidelines and frameworks. Specific proposals for revising MDCG guidance and promoting open-access initiatives are presented, demonstrating the project's commitment to fostering trust and compliance in CMDs.

Finally, **Chapter 5** provides the **Conclusions**, summarising key insights and outlining the next steps for advancing the ENTRUST project's goals.

Funded by the Horizon Framework Programme of the European Union

2 Legal and Ethical Considerations

2.1 Privacy and Data Protection

This section examines the regulatory frameworks governing privacy and data protection, which are central to the ENTRUST project's objectives. While prior deliverables provided a foundational analysis of international treaties and EU legislation, this section delves into specific legal and ethical requirements that shape the project's compliance. Particular attention is given to the General Data Protection Regulation GDPR [4], the Data Act [5], and the European Health Data Space (EHDS) [6], which collectively guide the protection and governance of personal data within CMDs. To clarify, privacy and data protection, though often used interchangeably, are distinct concepts. Privacy safeguards individual autonomy and protects against unwarranted intrusion, as recognised in the Universal Declaration of Human Rights (1948) and the European Convention on Human Rights (1950) [7]. Data protection, formally recognised as a right in the Charter of Fundamental Rights of the EU (2000), governs the processing and security of personal data, focusing on appropriate handling irrespective of its privacy impact. These fundamental rights form the basis of legislation like the GDPR [4], which grants individuals rights and enforces strict compliance on data handlers. This section highlights how these laws support ENTRUST in protecting sensitive data while enabling innovation in CMDs.

2.1.1 General Data Protection Regulation

The (GDPR) [4], effective from 25 May 2018, replaced Directive 95/46/EC as the primary EU framework for personal data protection. The GDPR [4] aims to protect the fundamental rights and freedoms of individuals, particularly their right to personal data protection, while ensuring the free movement of such data across the EU. Its extensive scope ensures adaptability to technological advancements, making it a robust and forward-thinking legal framework for the digital age. As outlined in ENTRUST's Data Management Plan (D1.4) [1] and Reference Architecture Deliverables (D2.1 - Initial Release and D2.2 - Final Release) [2], [3], GDPR [4] compliance is a critical component of the project's design and implementation.

2.1.1.1 Scope and Applicability of the GDPR

The GDPR establishes a robust framework for personal data protection, characterised by its extensive material scope. Defined in Article 2, the material scope ensures GDPR's relevance to diverse data-processing scenarios, encompassing both traditional and technologically advanced systems. This inclusive approach reflects the regulation's commitment to safeguarding fundamental rights while adapting to the complexities of modern digital environments.

The GDPR [4] applies to two principal categories of data processing:

1. ***Processing of Personal Data Wholly or Partly by Automated Means***. This includes operations using automated systems like cloud computing or IoT devices, such as real-

Funded by the Horizon Framework Programme of the European Union

time data collection or analytics. The GDPR ensures these dynamic processes are covered, reflecting the complexities of the digital age.

2. ***Processing of Non-Automated Personal Data Forming Part of or Intended to Form Part of a Filing System***. The GDPR also applies to manual processing where personal data is systematically organised in filing systems, whether physical, digital, or hybrid, ensuring consistent protection across all formats.

A distinguishing feature of the GDPR is its technology-neutral stance, which ensures that its provisions remain applicable regardless of the tools or methodologies employed. By focusing on the essence of data-processing activities, the regulation retains its efficacy amidst evolving technological innovations such as artificial intelligence, blockchain, and advanced data-mining techniques. This adaptability supports seamless integration of legal requirements with emerging technologies.

For the GDPR to apply, two fundamental criteria must be satisfied:

1. **Qualification as Personal Data**: The data must meet the GDPR's definition of personal data, which encompasses information relating to an identified or identifiable individual. This broad definition captures data such as names, online identifiers, and even dynamic IP addresses.
2. **Data Processing**: The data must undergo processing operations, as defined by GDPR Article 4(2), such as collection, recording, organisation, storage, or erasure. The inclusion of manual operations in a filing system ensures consistency in applying GDPR standards.

The material scope mandates compliance across diverse entities and projects:

- **Digital Service Providers**: Companies processing data via automated systems, including those employing algorithms for predictive analysis or customer insights, must ensure GDPR adherence.
- **Traditional Organisations**: Entities relying on manual records are equally bound, demonstrating the GDPR's breadth in safeguarding data.
- **Research Projects**: Initiatives like ENTRUST, which engage in personal data processing, particularly in sensitive contexts like healthcare, must address GDPR compliance from inception, covering areas such as informed consent, anonymisation, and privacy-by-design measures.

2.1.1.2 Key Concepts of the GDPR

For a comprehensive understanding of the GDPR, it is essential to explore its foundational definitions and principles. These definitions, outlined in Article 4 of the GDPR, serve as the cornerstone for interpreting and applying the Regulation across various contexts.

Funded by the Horizon Framework Programme of the European Union

2.1.1.2.1 Personal Data

According to Article 4(1), "*personal data*" refers to any information related to an identified or identifiable natural person, known as the "*data subject*." Identification can occur directly (e.g., through a name or ID number) or indirectly (e.g., via online identifiers or unique combinations of characteristics). The GDPR adopts a broad interpretation, covering objective data (e.g., medical test results) and subjective data (e.g., opinions). Personal data includes traditional identifiers such as names and addresses, as well as modern digital markers like IP addresses, cookie identifiers, and geolocation data. Importantly, the format or medium—whether digital, paper-based, or audio—does not affect its classification as personal data.

To fully grasp the scope of "personal data", it is necessary to delve deeper into its four fundamental elements as defined by the GDPR:

- "Any Information" - The phrase "any information" illustrates the GDPR's broad interpretation. This includes objective data (e.g., test results) and subjective data (e.g., opinions), regardless of accuracy or completeness. Personal data can exist in any format, from text and images to biometric and audio records.
- "Relating to" - Data is considered "relating to" an individual if it provides a meaningful link to that person. Examples include medical records, employment details, or behavioural data collected through wearables. The context determines whether the relationship exists
- "Identified or Identifiable" - A person is "identified" if they can be singled out directly, such as by name or ID number. A person is "identifiable" if they can be distinguished indirectly through combinations of data points (e.g., IP addresses combined with geolocation data). The GDPR establishes a low threshold for identification, ensuring robust protections even for inferred identities.
- "Natural Person" - GDPR protections apply exclusively to living individuals. While deceased persons and legal entities are excluded, exceptions may apply if data about a deceased individual reveals personal information about living relatives or if corporate identifiers reveal natural persons' identities.
- Special Categories of Personal Data: Certain personal data, such as racial or ethnic origin, political opinions, religious beliefs, genetic data, and health information, are categorised as sensitive under Article 9(1). Processing such data is generally prohibited unless specific legal conditions are met, reflecting the GDPR's risk-based approach. For example, health data encompasses medical histories, diagnostic results, and even inferred information from fitness trackers.

Funded by the Horizon Framework Programme of the European Union

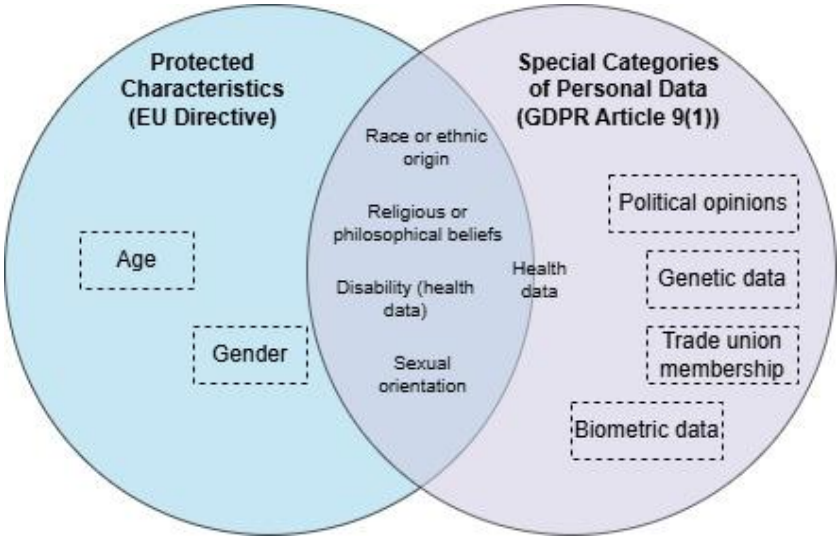

Figure 1: Diagram comparing Protected Characteristics (EU Directive) and Special Categories of Personal Data (GDPR Article 9(1))

2.1.1.2.2 Processing of Personal Data

The GDPR defines “processing” in Article 4(2) as any operation or set of operations performed on personal data, whether automated or not. This broad definition encompasses activities such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, dissemination, restriction, erasure, or destruction.

This broad definition ensures comprehensive protection for data subjects regardless of the techniques used. Key points regarding processing include:

- Automated processing: The GDPR applies automatically to any processing using technologies like computers or mobile devices.
- Manual systems: The GDPR applies to personal data in manual filing systems if the data is structured and accessible according to specific criteria.

Examples of processing under the GDPR relevant to the ENTRUST project include the collection, storage, transmission, and analysis of data from CMDs, encompassing health-related information and behavioural data. These activities qualify as personal data processing under the Regulation, ensuring GDPR compliance and safeguarding data subjects' rights throughout the project's data handling and trust assessment framework development.

2.1.1.2.3 Key Roles under the GDPR

- **Controller**

A “controller” is the entity that determines the purposes and means of processing personal data. Controllers may be individuals, legal entities, or public bodies, and they hold the primary responsibility for ensuring compliance with GDPR obligations. Decision-making power over the "why" and "how" of processing defines this role. For instance, within a consortium, controllers

Funded by the Horizon Framework Programme of the European Union

decide what data to collect, the lawful basis for processing, and the duration for which data is retained.

- **Processor**

A “processor” processes personal data on behalf of the controller. This role is limited to executing tasks determined by the controller and adhering to its instructions. Processors are bound by contractual agreements that stipulate their obligations, including maintaining data security, reporting breaches, and ensuring confidentiality. Processors may also engage sub-processors with explicit authorisation from the controller.

- **Joint Controllership**

Joint controllership arises when two or more entities jointly determine the purpose and means of processing. This relationship requires mutual arrangements to ensure GDPR compliance and shared accountability for data subject rights. Although levels of involvement may vary, joint controllers must formalise responsibilities through binding agreements.

- **Consent**

“Consent” under the GDPR is defined as any freely given, specific, informed, and unambiguous indication of a data subject’s agreement to the processing of their personal data. It can be provided through a written statement or clear affirmative action. For consent to be valid, it must be transparent and revocable at any time, ensuring the data subject retains control over their information.

- **Supervisory Authority**

A “supervisory authority” is a national data protection body responsible for enforcing GDPR compliance within its jurisdiction. These authorities oversee activities such as granting certifications, investigating breaches, and providing guidance on lawful processing practices. They also serve as a contact point for data subjects to lodge complaints or seek recourse for violations of their rights.

- **Relationship Between Controller and Processor**

The relationship between a controller and a processor is governed by GDPR Article 28. Controllers must ensure processors provide sufficient guarantees for implementing appropriate technical and organisational measures. This relationship is formalised through contracts that define the scope, duration, and nature of processing, as well as the respective rights and obligations of both parties.

2.1.1.3 General Principles of Data Protection and Rights of the Data Subjects under the GDPR

A responsible data controller must adhere to the principles outlined in GDPR Article 5 to ensure compliance and protect the personal data collected from individuals. These principles provide

Funded by the Horizon Framework Programme of the European Union

guidance for all entities required to be GDPR compliant and serve as a foundation for lawful data processing.

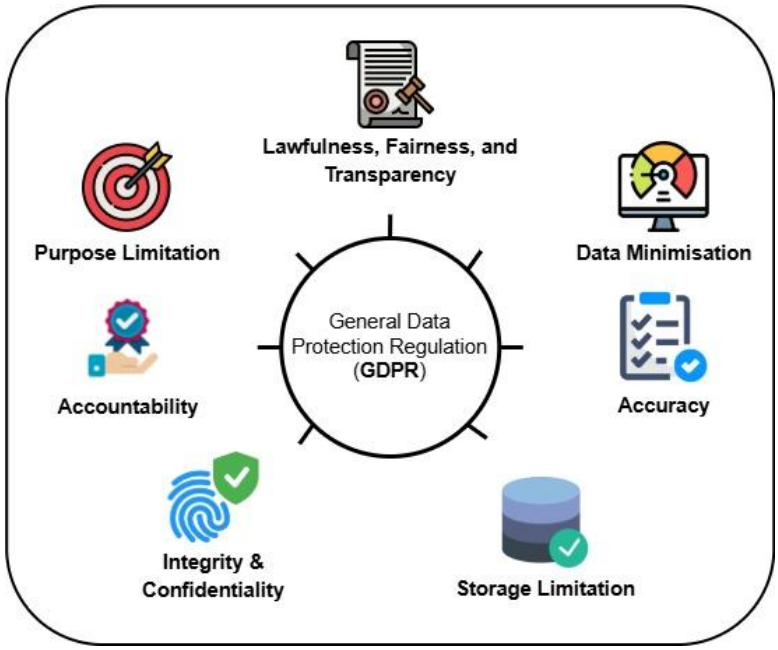

Figure 2: GDPR Principles

2.1.1.3.1 Key Principles of Data Processing

According to GDPR Article 5(2), the controller is accountable for, and must be able to demonstrate compliance with, the basic principles, which include:

- **Lawfulness, Fairness, and Transparency** - Data must be processed lawfully, fairly, and transparently. Lawful processing requires valid legal grounds, such as consent (Article 6), performance of a contract, or compliance with legal obligations. Fairness encompasses ethical considerations, requiring clear communication with data subjects about data collection and processing. Transparency mandates clear communication about what data is collected, why, and how it will be processed.
- **Purpose Limitation** - Personal data should be collected for specified, explicit, and legitimate purposes and not further processed in ways incompatible with those purposes. Exceptions include further processing for scientific or statistical purposes under Article 89(1), provided appropriate safeguards are in place.
- **Data Minimisation** - Data collection and processing must be limited to what is necessary for the intended purposes. This includes assessing the necessity of each data category collected and employing methods such as pseudonymisation.
  - *Anonymous and Pseudonymised Data* – It is important to clarify the distinction between anonymous and pseudonymised data, as these privacy-enhancing techniques play a crucial role in data protection. Pseudonymised data retains

Funded by the Horizon Framework Programme of the European Union

identifiers that allow re-identification with supplementary information, keeping it within the GDPR's scope. In contrast, anonymised data undergoes irreversible changes, ensuring it cannot be linked back to individuals and, therefore, falls outside GDPR regulation once fully anonymised. Techniques like pseudonym replacement, encryption, and randomisation help protect data, with pseudonymisation specifically recognised as a security measure under Articles 25 and 32 of GDPR.

- **Accuracy** - Controllers must ensure personal data accuracy and promptly rectify or delete inaccuracies to maintain trust and compliance.
- **Storage Limitation** - Personal data must not be retained longer than necessary for the purposes for which it was collected, except when required for archiving or research purposes under Article 89(1).
- **Integrity and Confidentiality** - Data must be securely processed to protect against unauthorised or unlawful access, loss, or damage through technical measures like encryption and organisational measures such as access controls.
- **Accountability** - Controllers must demonstrate compliance, maintain detailed records of processing activities, and adopt measures such as Data Protection Impact Assessments (DPIAs) to manage risks.

2.1.1.3.2 Legal Bases for Processing Personal Data

The GDPR mandates that personal data may only be processed if justified by at least one of the six lawful bases enumerated in Article 6(1). These lawful grounds ensure adherence to the principle of lawfulness and require controllers to identify, document, and communicate the basis for processing in their privacy notices. Controllers must evaluate each processing activity to select the most appropriate legal ground, considering the specific context.

The lawful grounds are:

1. **Consent (Art. 6(1)(a))**: Consent must be freely given, specific, informed, and unambiguous. GDPR Recitals 42 and 43 [4] underscore the importance of genuine choice, allowing individuals to refuse or withdraw consent without detriment. Consent must be specific to each processing purpose and communicated in clear, plain language. Pre-ticked boxes or silence do not constitute valid consent. Furthermore, controllers must demonstrate that the data subject has consented to the processing. For sensitive data, explicit consent is required under Article 9(2)(a). Withdrawal of consent must be as straightforward as granting it, and the withdrawal does not retroactively affect prior processing.
2. **Contract (Art. 6(1)(b))**: Processing is lawful when necessary to fulfil a contract with the data subject or to take pre-contractual steps at their request. This is particularly relevant for delivering goods, services, or employment-related obligations.

Funded by the Horizon Framework Programme of the European Union

3. **Legal Obligation (Art. 6(1)(c))**: Processing is required to comply with legal obligations, such as reporting or retaining data mandated by national or EU law. The specific purpose of processing must be determined by the law.
4. **Vital Interests (Art. 6(1)(d))**: Processing is justified when necessary to protect the vital interests of the data subject or another person, such as in emergencies where life or health is at stake.
5. **Public Task (Art. 6(1)(e))**: Processing is necessary for performing a task in the public interest or exercising official authority vested in the controller. The task must be grounded in EU or Member State law, which specifies the purpose of processing.
6. **Legitimate Interests (Art. 6(1)(f))**: Processing is permitted if it serves legitimate interests pursued by the controller or a third party, provided these interests do not override the rights and freedoms of the data subject. A balancing test is required to assess these interests, particularly in cases involving vulnerable individuals, such as children.

2.1.1.3.3 Record of Data Processing Activities

Another essential requirement under GDPR is maintaining records of processing activities, as outlined in Article 30. These records must document the purpose of processing, categories of personal data and data subjects, recipients, retention periods, and technical security measures. Although smaller organisations may be exempt, this requirement is strongly recommended for compliance and risk assessment purposes. Templates provided by national DPAs can assist with these documentation needs.

2.1.1.3.4 Data Management and Measures in ENTRUST

The ENTRUST project adopts a comprehensive and GDPR-compliant framework for managing personal data, as outlined in D1.4 Data Management Plan V2 [1], ensuring security, minimisation, and transparency at all stages of its operations. Key measures include:

- **Data Processing Principles**: Personal data collection and processing adhere to the principles of lawfulness, fairness, and transparency. Whenever possible, anonymisation is used to protect participant identities. Pseudonymisation may be applied when processing is necessary, with explicit consent obtained under GDPR Article 6 [4]. Data subjects are informed of data usage, and confidentiality is maintained unless compelling reasons dictate otherwise.
- **Data Minimisation**: Only the minimum necessary personal data is collected and processed for the project's specific objectives. De-identification techniques, such as anonymisation and pseudonymisation, are employed to reduce identification risks. Repurposing data is allowed only under strict conditions aligned with GDPR Article 5, ensuring compatibility with the initial purpose.

Funded by the Horizon Framework Programme of the European Union

- **Security of Processing**: Advanced security measures, including encryption, scrambling, and pseudonymisation, are implemented to prevent unauthorised access and ensure data integrity. The project ensures availability and accessibility of data in the event of physical or technical incidents and regularly tests and evaluates the effectiveness of security measures.
- **Data Breach Notification**: In compliance with GDPR Article 33, the project promptly notifies the supervisory authority within 72 hours of a personal data breach unless the breach poses minimal risks. Notifications include a description of the breach, affected data subjects, potential consequences, and mitigation measures.

By integrating these principles, ENTRUST ensures ethical, secure, and transparent management of personal data, fostering trust among participants and stakeholders.

2.1.1.3.5 Rights of Data Subjects

GDPR provides individuals with eight fundamental rights to ensure transparency, accountability, and control over their personal data:

- Right to Information and Access (Articles 12, 13, and 15) - Data subjects can access their personal data and understand how it is being processed.
- Right to Rectification (Article 16) - Data subjects can request corrections to inaccurate or incomplete personal data.
- Right to Erasure or 'Right to be Forgotten' (Article 17) - Individuals can request data deletion when no longer necessary for processing or other specific conditions apply.
- Right to Restriction of Processing (Article 18) - Processing can be restricted in cases like accuracy disputes or when data is no longer needed but cannot yet be erased.
- Right to Data Portability (Article 20) - Data subjects can transfer their data between controllers in a structured, machine-readable format.
- Right to Object (Article 21) - Individuals can object to data processing for certain purposes, such as direct marketing or profiling.
- Right Not to Be Subject to Automated Decision-Making, Including Profiling (Article 22) - Data subjects have the right to avoid decisions made solely through automated processing, unless exceptions like explicit consent or contractual necessity apply.
- Right to Lodge a Complaint - Individuals can file complaints with supervisory authorities if their rights are infringed.

2.1.1.3.6 Profiling and Automated Decision-Making

Profiling involves automated processing of personal data to categorise individuals or predict behaviour, preferences, or health outcomes. While beneficial in healthcare (e.g., precision medicine), profiling risks discrimination. GDPR Article 22 prohibits decisions based solely on automated processing that produce significant effects, except when based on explicit consent or

Funded by the Horizon Framework Programme of the European Union

legal grounds. Controllers must implement safeguards, such as algorithmic audits and mechanisms for human intervention.

2.1.1.3.7 Data Protection Officer (DPO)

Under GDPR Article 37, a DPO must be appointed in cases involving large-scale processing of sensitive data, regular monitoring of data subjects, or public authorities. The DPO oversees compliance, acts as a point of contact for supervisory authorities, and promotes a data protection culture.

2.1.1.3.8 Data Protection Impact Assessments (DPIA)

A DPIA, required under GDPR Article 35, identifies and mitigates risks to data subjects' rights from high-risk processing activities, such as large-scale processing of sensitive data or use of innovative technologies. The DPIA must include:

- A systematic description of the processing operations.
- An assessment of necessity and proportionality.
- Identification of risks to data subjects.
- Measures to mitigate these risks.

2.1.1.3.9 Notification of Data Breaches

GDPR Article 33 mandates notification to the supervisory authority within 72 hours of a personal data breach unless unlikely to risk individual rights. High-risk breaches also require prompt communication to affected individuals. Controllers must maintain robust breach detection and reporting procedures to comply effectively.

2.1.2 European Health Data Space

In May 2022, the European Commission (EC) published the legislative proposal for a Regulation for the EHDS, marking a significant step toward creating a unified framework for managing and sharing electronic health data across the European Union. The EHDS serves as a cornerstone of the broader European Health Union, aiming to enhance the accessibility, interoperability, and utility of health data while upholding the highest standards of privacy and security. Building upon and complementing key EU regulations, the EHDS integrates with the GDPR, which provides the foundational principles for data protection. It aligns with Regulation (EU) 2017/745 on Medical Devices (MDR) [8] and Regulation (EU) 2017/746 [9] on In Vitro Diagnostic Medical Devices (IVDR) [8], both of which define safety and performance standards for medical devices. Furthermore, the EHDS works in synergy with the proposed Artificial Intelligence Act and Data Act, which seek to regulate artificial intelligence and data sharing across various sectors. The EHDS establishes legal, technical, and governance structures to enable the effective primary use of electronic health data, such as its application in direct patient care, and secondary use, including research, innovation, and public policy. The overarching objective is to empower

Funded by the Horizon Framework Programme of the European Union

individuals with greater control over their health data while fostering innovation and collaboration within the health sector.

2.1.2.1 Overview and Applicability

The EHDS seeks to establish a unified framework for the secure and efficient management of electronic health data across the European Union. This ambitious initiative extends to manufacturers, suppliers, and users of electronic health record (EHR) systems and wellness applications, requiring them to adhere to strict standards of interoperability and data security. It also applies to healthcare providers, researchers, and policymakers engaged in processing health data responsibly.

2.1.2.1.1 Definition of Health Data Categories

Electronic health data under the EHDS is categorised into personal and non-personal data. Personal electronic health data includes information such as health and genetic data, as defined under the GDPR, and any data related to healthcare service provision. Non-personal data comprises anonymised or aggregated health information used for research, policy-making, or broader societal purposes.

2.1.2.1.2 Core Dimensions: Primary and Secondary Data Use

The EHDS establishes two distinct pathways for health data utilisation: **direct patient care** and **broader societal applications**.

- **Patient-Centric Data Use**: Primary use involves leveraging electronic health data for delivering healthcare services. This includes activities such as medical diagnosis, treatment, prescription, and managing reimbursement systems. By aligning with GDPR, the EHDS empowers patients to access, share, and manage their health records across Member States, ensuring seamless healthcare delivery.
- **Beyond the Patient - Wider Societal Goals:** Secondary use permits data processing for research, public health policy, and innovation. While enabling significant societal advancements, such data use must prioritise privacy by mandating pseudonymisation and prohibiting misuse for commercial activities like marketing or insurance calculations.

2.1.2.2 Governance and Operational Framework

The EHDS framework mandates the establishment of Health Data Access Bodies in each Member State to ensure adherence to its provisions. These entities are responsible for overseeing requests for secondary data use, acting as compliance regulators, and facilitating controlled access to datasets. Additionally, the EHDS introduces two pan-European platforms—MyHealth@EU and HealthData@EU—designed to enable secure, cross-border data exchange. MyHealth@EU supports healthcare providers and patients, while HealthData@EU focuses on researchers and policymakers, fostering collaboration and innovation. Furthermore, the EHDS imposes certification and technical compliance requirements on manufacturers of EHR systems

Funded by the Horizon Framework Programme of the European Union

and wellness applications. These include adherence to standards outlined in Annex II, such as robust data security protocols, logging mechanisms for data access, and patient-centric features like emergency access and data-sharing controls.

2.1.2.3 Emerging Concerns and Challenges

The EHDS represents a transformative initiative in health data governance within the European Union, offering significant opportunities for enhanced management and utilisation of electronic health data. However, the proposal has raised several considerations among stakeholders. The EHDS provides patients with greater control over their health data, including the ability to restrict access, which supports self-determination. Nevertheless, this provision may create challenges for healthcare providers, potentially resulting in gaps in critical information that could affect the quality of care and raise liability concerns. Additionally, healthcare professionals are likely to encounter increased administrative responsibilities due to the EHDS's robust data-sharing obligations, which might lead to legal ambiguities and potential conflicts with established ethical and confidentiality frameworks. Moreover, the EHDS must operate within the broader EU regulatory landscape, integrating seamlessly with existing frameworks such as GDPR, MDR, IVDR, and the proposed Artificial Intelligence (AI) Act [10]. While the proposal addresses certain overlaps, stakeholders have identified areas requiring further clarity to ensure consistent and coherent application across these regulatory frameworks. These elements highlight the importance of balancing the EHDS's ambitious objectives with practical implementation considerations.

2.1.2.4 Prospects for Transformation

The EHDS is poised to revolutionise the healthcare landscape by empowering patients, fostering innovation, and enhancing cross-border healthcare integration. A cornerstone of this transformation is the emphasis on patient autonomy. By granting individuals control over their health data, the EHDS strengthens transparency and trust in healthcare systems across the European Union. This empowerment aligns with the broader goal of fostering patient-centric healthcare delivery.

In addition to patient-focused initiatives, the EHDS facilitates innovation through the secondary use of health data. Researchers, policymakers, and innovators gain access to rich datasets that can drive advancements in medical research, public health strategies, and AI-powered healthcare applications. This focus on leveraging data for societal benefit underscores the EHDS's potential to catalyse technological and scientific breakthroughs, paving the way for more effective and efficient healthcare systems.

Another significant aspect of the EHDS is its commitment to unified cross-border care. Enhanced interoperability standards ensure seamless data exchange across Member States, simplifying access to health records for patients and providers alike. This facilitates greater patient mobility

Funded by the Horizon Framework Programme of the European Union

and continuity of care in transnational contexts, addressing one of the longstanding barriers to healthcare integration in the EU.

The proposal also addresses critical cybersecurity and regulatory considerations, especially concerning medical devices that may qualify as EHR systems. Manufacturers of such devices will need to comply with stringent security requirements outlined in Annex II of the EHDS, which include robust data protection protocols, access logging, and emergency access mechanisms. These provisions are designed to ensure that medical devices not only meet safety standards but also integrate seamlessly into the EHDS framework, aligning with broader regulatory initiatives such as the MDR.

While the EHDS holds significant promise, its ongoing legislative process leaves room for refinement. The interplay with existing frameworks such as GDPR, MDR, and the proposed Artificial Intelligence Act highlights the need for regulatory coherence. Nonetheless, the EHDS represents a pivotal step toward a more integrated and innovative healthcare ecosystem, aiming to balance individual rights, technological progress, and healthcare quality across the EU.

2.1.3 European Data Governance Act

The **European Data Governance Act (DGA)** [11] is a cornerstone of the European Union's data strategy, aiming to create a trusted, secure, and efficient framework for data sharing across the EU. Adopted in June 2022 and applicable since September 2023, the DGA is pivotal in unlocking the economic and societal potential of data while ensuring alignment with EU values, including transparency, privacy, and ethical use. This regulation addresses critical barriers to data sharing and lays the groundwork for the development of an integrated data-driven ecosystem across diverse sectors.

2.1.3.1 Objectives and Strategic Vision

The DGA seeks to:

- **Build Trust in Data Sharing**: By implementing robust legal and technical safeguards, the DGA addresses concerns around misuse of data and loss of competitive advantage. It emphasises neutrality and transparency to foster trust among stakeholders.
- **Increase Data Availability**: The regulation facilitates the reuse of both personal and non-personal data, opening avenues for innovation in sectors like healthcare, mobility, agriculture, and energy.
- **Foster Cross-Border Data Flows**: Through its structured framework, the DGA encourages seamless and secure data exchanges across Member States, promoting collaboration and the creation of Common European Data Spaces.

These goals are achieved through the DGA's focus on key mechanisms, such as data intermediation services, data altruism, and structured reuse of protected public sector data.

Funded by the Horizon Framework Programme of the European Union

2.1.3.2 Mechanisms of Implementation

The DGA introduces several measures to streamline and secure data sharing:

1. **Reuse of Protected Public Sector Data**: The DGA extends the Open Data Directive by enabling the reuse of protected data—such as personal or commercially sensitive information—that cannot be made openly available. Public sector bodies must implement tools like anonymisation, pseudonymisation, and secure processing environments to ensure privacy and confidentiality. For instance, health data held by public sector bodies can now be securely reused to advance research in rare diseases or improve public health responses, subject to stringent safeguards.
2. **Data Intermediation Services**: The regulation establishes neutral data intermediaries to act as trusted facilitators between data holders and data users. These entities operate under strict neutrality and transparency rules, ensuring that they do not directly use the data they manage for financial gain. This approach mitigates risks associated with monopolistic control by major tech platforms and enhances trust in the data-sharing ecosystem. Companies engaging in intermediation services must meet high compliance standards and are recognised as “data intermediation services providers” within the EU, further strengthening accountability.
3. **Data Altruism**: The DGA introduces mechanisms to encourage individuals and organisations to voluntarily share data for societal benefit, such as in healthcare, environmental sustainability, or mobility. Recognised data altruism organisations must operate on a not-for-profit basis and adhere to transparency and security requirements. This system allows for the creation of large, cross-border datasets that can drive advanced analytics and machine learning applications.
4. **European Data Innovation Board (EDIB)**: To harmonise practices and ensure cross-sectoral alignment, the EDIB develops guidelines on data intermediation, data altruism, and cross-border data sharing. This board also prioritises interoperability standards, essential for seamless data integration across Member States.

2.1.3.3 Societal and Economic Impact

The DGA’s holistic approach to data governance is expected to generate wide-ranging benefits:

- **For Citizens**: Enhanced access to public services, personalised healthcare, and better policy outcomes derived from data-driven decision-making.
- **For Businesses**: Lower costs of data acquisition and integration, accelerated innovation cycles, and the creation of novel data-driven products and services.
- **For Society**: Improved responses to challenges like climate change and pandemics, facilitated by better data access and analysis.

Funded by the Horizon Framework Programme of the European Union

For instance, in healthcare, the DGA's provisions can improve personalised treatments and enable quicker research advancements, saving billions in healthcare costs annually.

2.1.3.4 Relevance to the ENTRUST Project

The DGA has significant implications for the **ENTRUST project**, which focuses on building trust in digital healthcare systems, particularly CMDs. By leveraging the DGA's framework, ENTRUST can enhance its efforts in several areas:

1. **Dynamic Trust Assessment**: The DGA's emphasis on trust aligns directly with ENTRUST's goals. By utilising data intermediation services and data altruism mechanisms, the project can create secure channels for CMD data sharing that adhere to DGA standards.
2. **Cybersecurity Compliance**: ENTRUST's focus on security-by-design aligns with the DGA's stringent requirements for the secure reuse of data. The integration of anonymisation and secure processing tools complements ENTRUST's aim of safeguarding sensitive health data.
3. **Interoperability and Standardisation**: The DGA's interoperability mandates support ENTRUST's objective of creating seamless data flows between CMDs and healthcare systems. These provisions facilitate the development of cross-border solutions for healthcare monitoring and diagnostics.
4. **Sector-Specific Data Spaces**: The establishment of Common European Data Spaces, including a dedicated space for healthcare, provides ENTRUST with a structured environment to validate its trust assessment frameworks and pilot innovative use cases.

2.1.3.5 Challenges and the Path Ahead

While the DGA is a transformative step, its implementation poses challenges such as ensuring technical readiness, achieving regulatory coherence, and fostering widespread adoption among stakeholders. For ENTRUST, navigating these complexities will require close collaboration with policymakers and alignment with evolving standards.

By leveraging the DGA's principles, ENTRUST is well-positioned to advance its mission of fostering trust in healthcare digital transformation. The project can act as a model for how data governance policies translate into tangible societal benefits, driving innovation while safeguarding ethical and legal standards.

2.1.4 Data Act

The Data Act [5] was published in the Official Journal of the EU on 22 December 2023, and it will become applicable on 12 September 2025. The Data Act represents a pivotal regulation within the EU's data strategy, aiming to address challenges and unlock opportunities presented by industrial data. By establishing harmonised rules for data access, sharing, and portability, the Act

Funded by the Horizon Framework Programme of the European Union

seeks to create a fair, transparent, and innovative data economy. Its provisions hold particular relevance for the ENTRUST project, which aims to foster trust in CMDs by addressing legal, ethical, and technical challenges in the dynamic healthcare ecosystem.

2.1.4.1 Scope and Applicability

The Data Act establishes a comprehensive framework applicable across all economic sectors, providing harmonised rules for fair and secure access, sharing, and use of data. Its provisions apply horizontally, ensuring relevance to industries including manufacturing, agriculture, healthcare, and public services, while fostering innovation and competitiveness within the European data economy.

2.1.4.1.1 Sectoral Breadth

The Act covers data generated by Internet of Things (IoT) devices and related services, enabling data sharing and access in a secure and regulated manner. This includes personal and non-personal data, aligning with the GDPR while extending to non-personal data to ensure comprehensive governance. The Data Act supports seamless interoperability and equitable data-sharing mechanisms, particularly in dynamic and interconnected digital ecosystems.

2.1.4.1.2 Key Areas of Application

Under **Article 1(1)**, the Data Act addresses critical aspects of data accessibility and usage:

- **Making data and metadata available** to users of connected products and related services, ensuring user control over generated data.
- **Facilitating the transition** between data processing services, enhancing flexibility and competitiveness in the digital market.
- **Mandating data sharing** by data holders with recipients under transparent and fair conditions.
- **Providing public sector bodies** access to data for public interest tasks, particularly during emergencies or exceptional circumstances.

2.1.4.1.3 Stakeholders Covered by the Regulation

Article 1(2) specifies a wide range of stakeholders under the Act's scope:

- **Manufacturers of connected products** and providers of related services operating within the EU, regardless of their location.
- **Users**, both individuals and businesses, who interact with connected products or services and are empowered to control their data.
- **Data holders**, responsible for managing and sharing data generated by connected devices, ensuring compliance with user requests and legal requirements.
- **Public sector bodies** and EU institutions, which may access data for tasks of public interest under specific conditions.

Funded by the Horizon Framework Programme of the European Union

- **Providers of data processing services**, ensuring seamless interoperability and secure transitions between service providers.
- **Participants in data spaces and vendors of smart contracts**, fostering secure and transparent data-sharing agreements.

2.1.4.1.4 Definitions of Connected Products and Related Services

To ensure clarity, the Act defines connected products as items that generate, collect, or communicate data concerning their use or environment. These products must have primary functions unrelated to storing, processing, or transmitting data for third parties. Examples include medical devices (e.g., insulin pumps, wearable monitors), consumer electronics (e.g., smart home appliances), and industrial equipment (e.g., connected factory machinery).

Related services are digital services directly tied to the operation of connected products, enabling or enhancing their functionality. These include apps for monitoring performance, updating software, or sending operational commands. Services unrelated to the core operation of connected devices, such as auxiliary analytics or financial tools, fall outside the scope of the Act.

2.1.4.1.5 Applicability Across Data Transactions

The Act defines roles and responsibilities for key stakeholders to ensure accountability in the data ecosystem:

- **Users**: Individuals or entities owning or renting connected products or services are granted the right to access and share data they generate.
- **Data Holders**: These entities must ensure data is accessible, interoperable, and shareable in compliance with user requests and regulatory obligations.
- **Public Sector Bodies**: These organisations can access data under defined conditions, particularly during public emergencies or for public interest purposes, while adhering to GDPR requirements for personal data.

2.1.4.1.6 Practical Applications and Alignment with ENTRUST

The Data Act plays a pivotal role in shaping a transparent, equitable, and secure data-sharing ecosystem, directly influencing the implementation of connected products, including medical devices.

- **Interoperability and Portability** - The Act facilitates seamless data exchange across devices, services, and sectors, promoting integration in key domains such as healthcare, manufacturing, and smart cities. For medical devices, such as wearable monitors the Act ensures that data generated through their use is available to authorised users in structured, machine-readable formats. This enables stakeholders in healthcare ecosystems to derive actionable insights for personalised care and operational efficiency.

Funded by the Horizon Framework Programme of the European Union

In alignment with the ENTRUST project, this capability supports the integration of CMDs into dynamic trust assessment frameworks.

- **Enhanced Access for Public Interest** - The Data Act provisions allow public sector bodies to request data in exceptional circumstances, such as public health emergencies. This ensures timely access to crucial datasets for evidence-based policymaking and societal benefit. For example, during the COVID-19 pandemic, access to anonymised health data could have streamlined resource allocation and patient care. In the ENTRUST framework, these measures ensure that CMDs deployed in healthcare can contribute to public health objectives while maintaining compliance with GDPR and safeguarding individual privacy.

While the Data Act applies to a wide range of CMDs, the healthcare ecosystem presents unique complexities. The Act delineates roles and responsibilities for users, data holders, and public sector bodies, but challenges arise in defining these roles within the intricate value chains of healthcare. For instance:

- Patients often act as data subjects but may not be the direct users of connected devices, such as hospital-provided monitors.
- Healthcare organisations, such as hospitals, may serve as both users (in relation to manufacturers) and data holders (in relation to patients).
- Manufacturers of medical devices must ensure compliance with both the Data Act and the MDR, creating potential conflicts between user accessibility and cybersecurity obligations.

The ENTRUST project can leverage these provisions to explore ethical and regulatory dimensions of data sharing in healthcare, ensuring that CMDs are compliant with the Data Act while prioritising patient trust, privacy, and safety.

- **User Empowerment and Data Portability** - The Act ensures that users of connected devices—including healthcare providers and individual patients—have the right to access and share the data they generate. For ENTRUST, this aligns with efforts to build dynamic trust frameworks that empower patients and stakeholders to actively participate in their healthcare journeys. Additionally, the distinction between raw and derived data under the Act ensures that proprietary algorithms and intellectual property remain protected while enabling access to actionable data.
- **Fostering Competition and Innovation** - By requiring data holders to share data under fair and transparent conditions, the Act fosters an open and competitive market. Smaller entities and startups in healthcare technology benefit from reduced barriers to accessing data monopolised by larger organisations. This contributes to the ENTRUST project's objective of driving innovation in trustworthy digital healthcare solutions.

Funded by the Horizon Framework Programme of the European Union

2.2 Cybersecurity Regulations and Standards

The healthcare sector is increasingly targeted by cyberattacks, with incidents on hospital IT systems, electronic health records, and medical devices during the COVID-19 pandemic highlighting the urgency of enhanced cybersecurity. The digitalisation of healthcare has created new vulnerabilities, making it imperative to address cybersecurity challenges. Regulating this domain is complex, intersecting with the specialised and fragmented regulatory landscape of medical devices. The EU's cybersecurity framework spans multiple regulations, including the MDRIVDR, Cybersecurity Act (CSA) [12], Network and Information Systems Directive (NIS2) [13], GDPR, and Cyber Resilience Act (CRA) [14]. While these establish essential safeguards for CMDs, overlapping requirements create compliance challenges for manufacturers and healthcare providers. This section explores the EU's regulatory measures to enhance the cybersecurity of CMDs, addressing risks to data security and patient safety while aligning with Europe's digital transformation goals.

2.2.1 The Cybersecurity Act (CSA)

The CSA is a cornerstone regulation aimed at enhancing the EU's cybersecurity framework by strengthening the European Union Agency for Cybersecurity (ENISA) and establishing a unified certification framework for Information and Communication Technology (ICT) products, services, and processes. This dual-purpose legislation aims to bolster cybersecurity resilience and trust across the EU while fostering a harmonised digital market.

2.2.1.1 ENISA: A Strengthened Role

ENISA's role has been significantly expanded under the CSA, granting it a permanent mandate, additional resources, and enhanced responsibilities. As the EU's central authority on cybersecurity, ENISA provides critical support to Member States and EU institutions in managing and mitigating cyber risks. Its functions include assisting in the coordination of responses to large-scale cross-border cyberattacks, developing technical frameworks for cybersecurity certification, and serving as the secretariat for the CSIRTs Network established under the NIS Directive. In addition to its operational role, ENISA also supports the implementation of EU cybersecurity policies and laws by providing expert advice and building capacity among Member States. It plays a pivotal role in reducing regulatory fragmentation, harmonising cybersecurity standards, and informing the public about certification schemes through a dedicated platform. This expanded mandate positions ENISA as a key player in enhancing EU-wide cooperation on cybersecurity and fostering trust among stakeholders.

2.2.1.2 The European Cybersecurity Certification Framework

The CSA introduced the EU-wide cybersecurity certification framework to unify and simplify cybersecurity standards for ICT products, services, and processes. By establishing mutual recognition of certifications across Member States, the framework reduces administrative burdens

Funded by the Horizon Framework Programme of the European Union

and facilitates cross-border trade for companies operating in the EU. The certification framework defines clear assurance levels—basic, substantial, and high—based on the security needs of ICT products and their intended use. These levels allow stakeholders to understand the cybersecurity risk associated with a product or service, ranging from minimal to robust security standards. The framework's harmonised approach ensures consistent evaluation criteria, methodologies, and security objectives across the EU, fostering a cohesive and secure digital market. While certification under the framework is voluntary, it provides manufacturers and service providers with an opportunity to demonstrate their commitment to cybersecurity, thereby enhancing trust and competitiveness. Recent amendments to the CSA, proposed in April 2023, aim to expand the framework's scope to include managed security services, addressing evolving threats and ensuring the reliability of critical cybersecurity operations like incident response and security audits.

2.2.1.3 European Common Criteria-Based Certification Scheme (EUCC)

The CSA also established the **European Common Criteria-based Certification Scheme (EUCC)** [15], which builds on international standards for IT security. The scheme provides a comprehensive structure for evaluating the security of ICT products and processes and ensures compliance with the **Common Criteria** framework.

Features of the EUCC include:

- **Comprehensive Evaluation**: Detailed standards for evaluation, issuance, renewal, and withdrawal of certificates.
- **Transparency**: Clear obligations for manufacturers to provide guidance on maintaining product security.
- **Mutual Recognition**: Alignment with the **Mutual Recognition Agreement (MRA)** for IT security certificates.

The **EU Cybersecurity Certification Group (ECCG)** supports the implementation and maintenance of the scheme, ensuring collaboration between public and private stakeholders.

2.2.1.4 Implications for CMDs

For sectors like healthcare, the CSA offers a framework to certify **CMDs**, addressing key challenges such as:

- **Interoperability**: Ensuring CMDs meet standardised cybersecurity benchmarks.
- **Transparency**: Requiring manufacturers to provide security guidance and disclose known vulnerabilities.
- **Enhanced Resilience**: Building trust in medical devices through robust certification processes.

Funded by the Horizon Framework Programme of the European Union

By harmonising cybersecurity requirements, the CSA supports manufacturers in reducing compliance burdens and enhances patient safety by mitigating cyber risks. It aligns closely with initiatives like **ENTRUST**, where cybersecurity is integral to fostering trust in healthcare technologies.

2.2.2 The NIS 2 Directive

The Network and Information Security 2 (NIS2) Directive represents a significant evolution in the EU's cybersecurity framework, aiming to address the limitations of its predecessor, the NIS Directive of 2016. By modernising legal measures to match the growing digitisation and escalating cybersecurity threats, the NIS2 Directive establishes a comprehensive and harmonised approach to enhance the cybersecurity resilience of public and private entities across the EU. The Directive came into force in January 2023, and Member States must integrate it into their national legislation by October 2024.

2.2.2.1 Key Objectives and Scope

The NIS2 Directive seeks to bolster cybersecurity preparedness and cooperation among Member States while fostering a robust security culture across critical sectors of the EU economy and society. These sectors include energy, transport, healthcare, banking, digital infrastructure, and more. The Directive mandates:

- **Enhanced Preparedness:** Member States must establish or strengthen Computer Security Incident Response Teams (CSIRTs) and competent national authorities for network and information system security.
- **Cross-Border Cooperation:** The Directive establishes a Cooperation Group to facilitate strategic collaboration and information exchange among Member States.
- **Risk-Based Measures:** Essential and important entities in critical sectors are required to implement cybersecurity risk management and reporting mechanisms.

2.2.2.2 Expanded Scope and Categorisation

Compared to its predecessor, the NIS2 Directive significantly broadens its scope. It includes new sectors and entities deemed critical for economic and societal resilience, such as healthcare providers, manufacturers of medical devices, and entities in digital services and research. The Directive categorises entities into two groups:

1. **Essential Entities:** Organisations of high criticality, such as hospitals and pharmaceutical manufacturers, which must comply with stricter cybersecurity requirements.
2. **Important Entities:** Organisations of other critical sectors, such as manufacturers of in vitro diagnostic medical devices, which also fall under cybersecurity obligations but with slightly less stringent requirements.

Funded by the Horizon Framework Programme of the European Union

This expanded scope ensures that both public and private entities critical to the EU's functioning are covered, reducing inconsistencies across Member States.

2.2.2.3 Cybersecurity Risk Management Measures

Under Article 21(2) of the NIS2 Directive, entities must implement comprehensive cybersecurity risk management measures grounded in an all-hazards approach. These measures aim to safeguard both network and information systems and their physical environments from incidents. The measures include:

- Developing **policies for risk analysis and information system security** to identify and mitigate potential vulnerabilities effectively.
- Establishing robust **incident handling procedures** to manage and respond to cybersecurity events promptly.
- Ensuring **business continuity** through backup management, disaster recovery planning, and crisis management to minimise operational disruptions.
- Strengthening **supply chain security**, including assessing and managing cybersecurity risks associated with suppliers and service providers.
- Enhancing **security in the acquisition, development, and maintenance of network and information systems**, with emphasis on vulnerability handling and disclosure.
- Regularly assessing the **effectiveness of cybersecurity risk management measures** through structured policies and procedures.
- Promoting **basic cyber hygiene practices** and implementing ongoing **cybersecurity training** for staff.
- Implementing **policies for the use of cryptography** and encryption where appropriate to protect sensitive data.
- Securing **human resources and asset management**, with robust access control policies.
- Adopting advanced technologies such as **multi-factor authentication**, secure communication systems (voice, video, and text), and secure emergency communication protocols where necessary.

These measures integrate organisational, operational, and technical dimensions, ensuring a holistic and unified approach to managing cybersecurity risks.

2.2.2.4 Incident Reporting Obligations

The NIS2 Directive requires essential and important entities to notify national authorities promptly of any significant cybersecurity incidents. The reporting process, defined under Article 23, includes the following stages:

1. **Early Warning:** Within 24 hours of becoming aware of the incident, entities must issue an initial alert to relevant authorities, providing preliminary details of the breach.

Funded by the Horizon Framework Programme of the European Union

2. **Incident Notification:** A more detailed report must be submitted within 72 hours, outlining the nature, impact, and initial response measures taken.
3. **Final Report:** No later than one month after submitting the incident notification, a comprehensive report must be provided. This report should include a complete assessment of the incident, the actions taken to address it, and measures to prevent recurrence.

These reporting requirements ensure timely communication, enabling authorities to coordinate responses effectively while reinforcing accountability and transparency among affected entities.

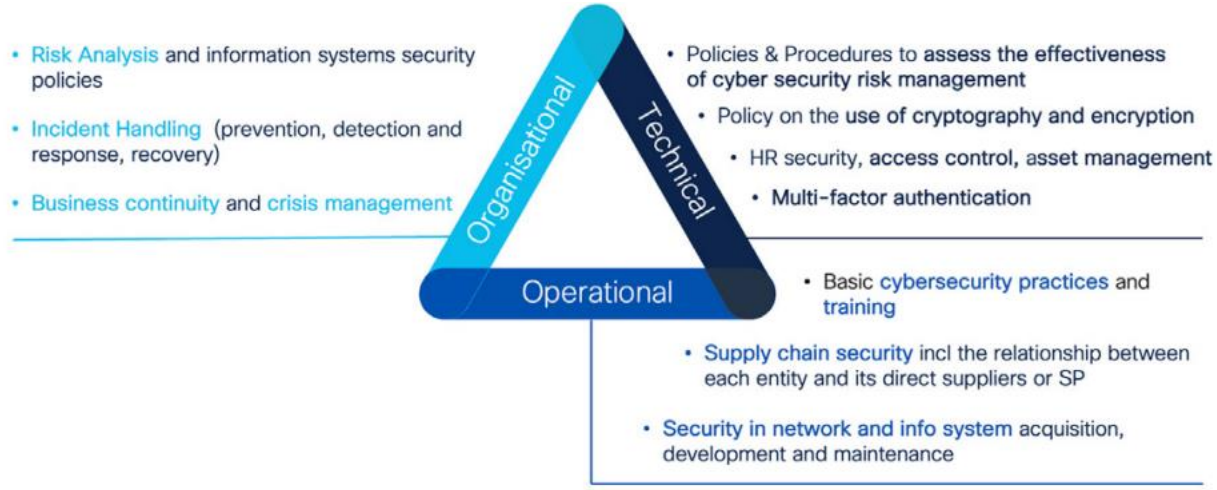

Figure 3: NIS 2 Risk Management. Source: CISCO White Paper, p17 [16].

2.2.3 Cyber Resilience Act (CRA)

The CRA [14] represents a transformative addition to the EU's cybersecurity legislative landscape. It introduces horizontal cybersecurity requirements for products with digital elements, addressing critical vulnerabilities and ensuring the security of these products throughout their lifecycle. By mandating compliance at every stage, from design and production to maintenance, the CRA aims to enhance trust in digital products and protect both consumers and businesses.

2.2.3.1 Objectives and Scope

Adopted in December 2024, the CRA seeks to harmonise cybersecurity standards for products with digital components, reducing fragmentation in the internal market. It aims to:

1. **Enhance Cybersecurity Resilience**: Requiring robust protection mechanisms for hardware and software products against known and emerging cyber threats.
2. **Ensure Lifecycle Security**: Mandating ongoing maintenance and updates to address vulnerabilities over the product's lifecycle.
3. **Empower Consumers**: Enabling buyers to make informed decisions by providing clear information on a product's cybersecurity features.

Funded by the Horizon Framework Programme of the European Union

The CRA applies to all products with digital elements that connect directly or indirectly to other devices or networks, including IoT devices, operating systems, and non-embedded software. Notably, it excludes products governed by specific sectoral regulations, such as medical devices (MDR/IVDR), and those developed exclusively for national security or military purposes.

2.2.3.2 Key Provisions

2.2.3.2.1 Essential Cybersecurity Requirements

Manufacturers must ensure that their products meet the cybersecurity requirements outlined in Annex I. These include:

- **Protection Against Unauthorised Access**: Products must incorporate authentication mechanisms, identity management systems, and access controls to prevent unauthorised use.
- **Data Confidentiality**: Data stored, transmitted, or processed by the product must be secured through encryption or equivalent state-of-the-art mechanisms.
- **Vulnerability Management**: Products must undergo regular security assessments, with mechanisms in place to identify, record, and mitigate vulnerabilities.
- **Lifecycle Support**: Manufacturers are obliged to provide free security updates and patches throughout the product's expected operational period.

These requirements ensure that products are resilient to cyber threats from their inception and throughout their use.

2.2.3.2.2 Transparency and Consumer Information

Manufacturers must supply clear, intelligible, and accessible instructions and information with their products. This documentation must include:

- Details on secure installation and maintenance.
- Guidelines on mitigating potential risks associated with the product's use.
- Instructions for applying security updates and patches.

This transparency fosters trust among consumers and businesses, helping them understand and manage cybersecurity risks effectively.

2.2.3.3 Reporting Obligations of Manufacturers

The **CRA** imposes stringent reporting requirements on manufacturers to ensure rapid response and mitigation of cybersecurity risks associated with products with digital elements. These obligations aim to enhance transparency and enable swift corrective actions to minimise the impact of cybersecurity incidents.

Funded by the Horizon Framework Programme of the European Union

2.2.3.3.1 Mandatory Notifications

Under **Article 14(1)(2)**, manufacturers are required to notify the **CSIRT** designated as the coordinator and **ENISA** upon becoming aware of any actively exploited vulnerabilities or severe incidents. The notification process follows a tiered timeline:

- **Early Warning Notification**:
  - Manufacturers must submit an early warning within **24 hours** of becoming aware of an actively exploited vulnerability.
  - This notification should provide preliminary information about the issue to allow for an immediate response.
- **Detailed Vulnerability Notification**:
  - A more comprehensive notification must follow within **72 hours**, including specifics about the vulnerability's nature, scope, and potential impacts.
- **Final Report**:
  - A detailed report must be submitted no later than **14 days** after implementing corrective or mitigating measures. This report should include:
    - A description of the vulnerability, its severity, and potential impacts.
    - Available information about any malicious actors exploiting the vulnerability.
    - Details of security updates or corrective measures provided to remedy the vulnerability.

These requirements ensure prompt communication with relevant authorities and stakeholders, facilitating swift containment and mitigation of cybersecurity threats.

2.2.3.3.2 Incident Reporting

In addition to vulnerabilities, manufacturers must notify authorities about **severe incidents** impacting the security of digital products within the same timelines as for vulnerability notifications. This includes providing early warnings, detailed incident notifications, and final reports outlining the resolution measures taken.

2.2.3.3.3 User Notifications

Manufacturers are obligated to inform affected users, and where appropriate, all users, about actively exploited vulnerabilities or severe incidents. Such notifications must include:

- Information on the nature of the vulnerability or incident.
- Risk mitigation advice and corrective measures users can take to minimise the impact.
- These communications should be provided in a structured, machine-readable format for ease of processing and implementation.

Funded by the Horizon Framework Programme of the European Union

2.2.3.3.4 Voluntary Notifications

Manufacturers, as well as other stakeholders, may voluntarily report vulnerabilities or cyber threats affecting the risk profile of a product with digital elements. These reports can be submitted to a CSIRT or **ENISA**, helping create a collaborative environment for enhancing cybersecurity across the EU.

2.2.3.3.5 Simplified Reporting Platform

To streamline the notification process, ENISA is tasked with establishing a **single reporting platform**. This centralised system will facilitate efficient submission and management of reports, reducing administrative burdens on manufacturers while ensuring timely action by relevant authorities.

The CRA's robust reporting framework underscores the importance of proactive communication in addressing cybersecurity risks, fostering greater trust and security in products with digital elements across the EU.

2.2.3.4 Conformity Assessment and Certification

The Cyber Resilience Act (CRA) establishes a robust framework for the conformity assessment and certification of products with digital elements. This framework ensures that such products meet stringent cybersecurity requirements before entering the EU market, enhancing trust and resilience across the digital ecosystem.

2.2.3.4.1 Conformity Assessment Procedures

Article 32 of the CRA outlines the conformity assessment process, which varies in complexity depending on the level of risk associated with the product. Manufacturers must demonstrate compliance with the cybersecurity obligations outlined in the CRA through one of the following pathways:

- **Internal Control Procedure (Module A)**:
    - A simplified process where the manufacturer internally verifies that the product meets the essential requirements outlined in Annex I of the CRA. This method is suitable for products with lower risk profiles.
- **EU-Type Examination Procedure (Module B) Combined with Internal Production Control (Module C)**:
    - A two-step process where an authorised body conducts an independent evaluation of the product's design (Module B), followed by internal production checks by the manufacturer (Module C).
- **Full Quality Assurance (Module H)**:

Funded by the Horizon Framework Programme of the European Union

- A comprehensive approach involving an in-depth review of the manufacturer's entire quality management system by a notified body. This method is typically required for high-risk products.

- **European Cybersecurity Certification Scheme**:
  - Where applicable, products may be certified under a relevant EU cybersecurity certification scheme, as per Article 27(9). This option provides an additional layer of assurance by adhering to an established certification framework.

2.2.3.4.2 Application of the CE Marking

Upon successful conformity assessment, manufacturers must draw up an EU Declaration of Conformity. This declaration confirms that the product meets the cybersecurity requirements of the CRA. Subsequently, the product is affixed with the CE marking, signifying compliance and granting it access to the EU market.

2.2.3.4.3 Alignment with High-Risk AI Systems

Products classified as high-risk AI systems under the Artificial Intelligence Act must also comply with the cybersecurity requirements specified in the CRA. An EU Declaration of Conformity issued under the CRA serves as evidence of compliance with the AI Act's cybersecurity provisions.

2.2.3.4.4 Compliance and Penalties

Non-compliance with the CRA can result in significant penalties, including fines of up to €15 million or 2.5% of the total annual global turnover, whichever is higher. This underscores the critical importance of adherence to the CRA's requirements, as failure to comply could lead to substantial financial and reputational damage.

2.2.3.4.5 Implications for Manufacturers

Manufacturers bear the primary responsibility for ensuring conformity with the CRA. This includes:

- Conducting a thorough assessment of cybersecurity risks associated with their products.
- Implementing measures throughout the product's lifecycle to mitigate risks and prevent incidents.
- Maintaining technical documentation and providing necessary information to users.

2.2.3.4.6 Role of Risk-Based Procedures

The CRA adopts a risk-based approach, tailoring the stringency of conformity assessments to the potential cybersecurity risks posed by the product. High-risk products, such as those critical to infrastructure or healthcare, undergo more rigorous evaluation processes to ensure enhanced security and reliability.

2.2.3.4.7 Ensuring Market Integrity

By mandating conformity assessments and certification, the CRA aims to harmonise cybersecurity standards across the EU. This ensures a unified approach to product safety,

Funded by the Horizon Framework Programme of the European Union

reduces market fragmentation, and enhances consumer confidence in digital products. Through this comprehensive framework, the CRA supports the development and deployment of secure products with digital elements, fostering a safer digital landscape for consumers and businesses alike.

2.2.3.5 Alignment with EU Strategies

The CRA aligns with the EU Cybersecurity Strategy (2020) and the EU Security Union Strategy, complementing legislation such as the NIS2 Directive. By harmonising rules and fostering a unified market for secure digital products, the CRA addresses critical cybersecurity gaps and strengthens the overall resilience of the EU's digital ecosystem. It sets a clear precedent for integrating cybersecurity into the design and development of all digital products, thereby enhancing trust and security in an increasingly interconnected world.

2.3 Regulatory Frameworks for Medical Devices

Technological advancements in healthcare have driven significant innovation in medical devices, introducing complex systems that include software, connectivity, and even artificial intelligence. To ensure safety, efficacy, and consistent quality across the EU, robust regulatory frameworks have been established. These frameworks include the MDR and the IVDR. These regulations are designed to harmonise standards across Member States, improve patient safety, and address challenges posed by technological integration in medical devices. The regulations also align with other EU legislative frameworks, including cybersecurity measures, recognising the critical importance of integrating robust security features in devices that are increasingly interconnected and data-dependent. Complementing the MDR and IVDR, the Medical Device Coordination Group (MDCG) provides targeted guidance to ensure manufacturers meet cybersecurity requirements, fostering resilience and trust in the rapidly evolving landscape of medical technologies. The following sections explore the MDR, IVDR, and the guidance provided by MDCG in detail, with an emphasis on how these regulations and guidelines collectively address the safety, performance, and cybersecurity of medical devices.

2.3.1 Medical Devices Regulation (MDR)

The Medical Devices Regulation (MDR), adopted in April 2017, represents a significant reform of the EU's regulatory framework for medical devices. Fully binding as of May 26, 2021, the MDR replaces the previous directives, the Medical Devices Directive (MDD) and the Active Implantable Medical Devices Directive (AIMDD), with a more stringent and harmonised approach to medical device safety and performance. This legislative overhaul addresses the rapid advancements in healthcare technology and the increasing complexity of devices, including software as a medical device (SaMD), connectivity, and artificial intelligence.

Funded by the Horizon Framework Programme of the European Union

2.3.1.1 Scope and Applicability

The MDR applies directly to all EU Member States, ensuring uniformity across the Union without requiring national transposition. It governs the placement on the market, availability, and use of medical devices for human use, including accessories. A **key principle** of the MDR is the **"intended purpose"** of a device as defined by the manufacturer, which determines whether it qualifies as a medical device under the regulation.

According to **Article 2(1)**, a medical device is defined as:

"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 one or more specific medical purposes..."

These purposes include:

- Diagnosis, prevention, monitoring, treatment, or alleviation of diseases or injuries.
- Investigation, replacement, or modification of anatomy or physiological processes.
- Providing diagnostic information via in vitro examination.

Accessories, as defined in **Article 2(2)**, are also included in the scope of the MDR, provided they enable or assist a medical device in fulfilling its intended medical purpose.

Products without a medical purpose but with similar risks, such as aesthetic devices (e.g., contact lenses or liposuction devices), are listed in **Annex XVI** and are subject to the MDR's provisions.

2.3.1.2 Key Provisions and Objectives

The MDR introduces several critical changes aimed at enhancing patient safety and strengthening public confidence in medical devices. These include:

- **Harmonisation Across the EU**: As a vertical legislative act, the MDR eliminates the fragmentation of previous directives by applying directly across Member States, ensuring consistency in medical device regulation.
- **Risk-Based Classification**: Devices are categorised into **Classes I, IIa, IIb, and III** based on the level of risk associated with their use. Higher-risk devices, such as implantable Class III devices, are subject to the most stringent requirements, including detailed clinical evaluations and independent assessments by Notified Bodies.
- **Lifecycle Approach to Safety**: The MDR emphasises the importance of device safety throughout its lifecycle, encompassing design, manufacturing, and post-market phases. Manufacturers must establish and maintain robust **risk management systems** that are continually updated to reflect the state of the art.
- **Clinical Evidence and Evaluation**: Clinical evaluations are now mandatory for all classes of devices, with stricter requirements for high-risk categories. The reliance on equivalence

Funded by the Horizon Framework Programme of the European Union

data has been limited, pushing manufacturers to conduct new clinical investigations to demonstrate compliance.

- **Post-Market Surveillance (PMS)**: Manufacturers are required to implement proactive PMS processes to monitor device performance, collect real-world data, and address safety concerns promptly. This includes **Post-Market Clinical Follow-Up (PMCF)**, ensuring clinical evaluations remain current.
- **Unique Device Identification (UDI)**: The MDR mandates the use of **Unique Device Identifiers (UDI)** to enhance traceability and facilitate monitoring through the **EUDAMED database**.

2.3.1.3 Software as a Medical Device (SaMD)

The MDR explicitly addresses software, recognising its growing role in healthcare. According to **Recital 19**, software qualifies as a medical device if it is intended for medical purposes, as outlined in the regulation. Standalone software or software driving a device may qualify as a medical device if it serves purposes such as diagnosis, monitoring, or treatment of disease. Conversely, software used for general purposes, lifestyle, or well-being does not fall under the MDR's scope.

The qualification of software as a medical device is determined by:

- The **manufacturer's intended purpose**.
- The software's functionality and role in achieving medical outcomes.

The **Medical Device Coordination Group (MDCG)** provides further guidance, including decision trees, to assist in classifying software under the MDR.

2.3.1.4 General Safety and Performance Requirements (Annex I)

The **MDR** mandates a comprehensive framework of **General Safety and Performance Requirements (GSPRs)** outlined in **Annex I**. These requirements establish the foundation for ensuring that all medical devices meet stringent safety, performance, and risk management standards before entering the EU market. Key obligations for manufacturers include the following:

- **Performance and Purpose**:
  - Devices must achieve the performance intended by their manufacturer and be designed to be safe, effective, and suitable for their intended medical purpose.
  - The benefits of device usage must outweigh the associated risks, considering the state of the art.
- **Risk Management System**:
  - Manufacturers are required to establish, implement, document, and maintain a comprehensive **risk management system** throughout the device lifecycle. This

Funded by the Horizon Framework Programme of the European Union

includes risk identification, mitigation strategies, and continuous updates to reflect evolving safety standards.

- **Interoperability and Compatibility**:
  - Devices intended for use with other equipment must ensure compatibility and safety without impairing their intended performance.
- **Software-Related Requirements**:
  - Devices incorporating electronic programmable systems or standalone software must be designed for **repeatability, reliability, and performance** in line with their intended use.
  - Software must be developed and maintained according to the state of the art, respecting principles of development lifecycle, risk management (including cybersecurity), verification, and validation.
- **Cybersecurity and IT Measures**:
  - Devices must include robust measures to protect against unauthorised access, data breaches, and potential cybersecurity risks. This includes establishing hardware, IT network characteristics, and security measures to safeguard data integrity and privacy.
- **State-of-the-Art Manufacturing and Design**:
  - Devices must adhere to state-of-the-art manufacturing and design principles, ensuring minimal risks from software-hardware interactions or IT environments.

2.3.1.5 Classification and Risk Management

The MDR adopts a **risk-based classification system** that considers the vulnerability of the human body and the potential risks associated with medical devices. Devices are divided into four classes as per **Article 51(1)**:

- **Class I**: Low-risk devices (e.g., bandages, reusable surgical instruments).
- **Class IIa**: Medium-risk devices (e.g., hearing aids).
- **Class IIb**: Medium-high-risk devices (e.g., ventilators, imaging systems).
- **Class III**: High-risk devices (e.g., pacemakers, heart valves).

2.3.1.5.1 Conformity Assessment Routes

- **Class I** devices are subject to self-certification by manufacturers.
- **Classes IIa, IIb, and III** require assessment and certification by **Notified Bodies**. Higher-risk devices (Class III) necessitate more rigorous evaluations, including clinical trials and independent expert reviews.

Funded by the Horizon Framework Programme of the European Union

2.3.1.5.2 CE Marking and Compliance

To achieve **CE marking**, manufacturers must:

- Implement a **Quality Management System (QMS)**.
- Provide extensive technical documentation for development and manufacturing processes.
- Conduct a **clinical evaluation** demonstrating device safety and efficacy, ensuring the benefits outweigh potential risks.

2.3.1.6 Clinical Data, Post-Market Surveillance, and Incident Reporting

- **Clinical Evaluation Requirements**:
  - All devices must undergo a clinical evaluation, with high-risk devices (Class III and some Class IIb) requiring more stringent clinical investigations.
  - Evaluations must align with state-of-the-art practices, ensuring safety and performance.
- **PMS**:
  - Manufacturers must establish active and systematic PMS processes to collect real-world data, monitor device performance, and address safety concerns promptly.
  - **PMCF** is required to keep clinical evaluations up-to-date.
- **Incident Reporting**:
  - Under **Article 87(1)**, manufacturers must report serious incidents involving their devices to the relevant competent authorities.
  - Serious incidents include:
    - Death or serious health deterioration of a patient or user.
    - Public health threats.

Reporting timelines are proportional to the incident severity:

- **Immediately** and no later than 15 days for serious incidents.
- **Within 2 days** for serious public health threats.

This comprehensive framework ensures that medical devices are safe, effective, and continuously monitored, fostering trust among users and compliance with EU standards.

2.3.2 In Vitro Diagnostic Medical Devices (IVDR)

The **IVDR** (EU 2017/746) establishes a comprehensive regulatory framework for in vitro diagnostic (IVD) medical devices, ensuring high standards of quality, safety, and performance. Adopted on **April 5, 2017**, the IVDR replaced the previous Directive 98/79/EC on **May 26, 2022**, after a five-year transitional period. Unlike its predecessor, the IVDR is directly applicable across

Funded by the Horizon Framework Programme of the European Union

all EU Member States without requiring national transposition, contributing to regulatory harmonisation and market uniformity.

2.3.2.1 Scope and Purpose

The IVDR applies to a wide range of IVD medical devices, including reagents, calibrators, control materials, instruments, software, and specimen receptacles. These devices play a crucial role in healthcare by examining specimens from the human body to provide information on:

- Physiological or pathological processes or states.
- Congenital physical or mental impairments.
- Predispositions to medical conditions or diseases.
- Compatibility with potential recipients.
- Prediction of treatment responses or reactions.
- Definition or monitoring of therapeutic measures.

The regulation aims to safeguard public health and patient safety while ensuring the smooth functioning of the internal market. It acknowledges the contribution of small and medium-sized enterprises (SMEs) in this sector and seeks to maintain their active participation.

2.3.2.2 Key Changes Introduced by the IVDR

The IVDR introduces several significant changes compared to the previous Directive:

- **Expanded Scope and Increased Oversight**: Under Directive 98/79/EC, only about 8% of IVD devices underwent oversight by notified bodies. With the IVDR, approximately **80%** of devices now require independent conformity assessment, significantly increasing scrutiny over device safety and performance.
- **Risk-Based Classification System**: Following a structure similar to the MDR, devices are classified based on their intended purpose and inherent risks, ensuring a proportionate level of regulatory control. Classes range from low-risk to high-risk, with higher-risk devices requiring stricter conformity assessments.
- **Rules for In-House Devices**: The IVDR establishes common rules for in-house devices used within health institutions. These include justification for use, compliance with safety and performance standards, and the implementation of appropriate quality management systems.
- **Enhanced General Safety and Performance Requirements**: The IVDR outlines detailed requirements for device design, manufacturing, and intended use. These are similar to the **General Safety and Performance Requirements** (Annex I) under the MDR, focusing on ensuring device reliability and minimising associated risks.

Funded by the Horizon Framework Programme of the European Union

- **Conformity Assessment Procedures**: The regulation strengthens the role of notified bodies, requiring conformity assessments for most IVD devices. This involves evaluations of design, clinical evidence, and quality management systems, ensuring robust oversight.

2.3.2.3 Harmonisation with MDR

The IVDR aligns closely with the **MDR** (EU 2017/745) in structure and logic. Both aim to increase patient safety by enhancing device quality and performance. Shared features include:

- A risk-based classification system.
- Detailed general safety and performance requirements.
- The requirement for manufacturers to maintain lifecycle risk management systems.
- Common rules for cybersecurity and data protection.

Although their scopes differ—MDR covering medical devices and IVDR focusing on in vitro diagnostics—both regulations converge on key principles, including cybersecurity. For simplicity, cybersecurity requirements discussed in the MDR section apply similarly to IVD devices under the IVDR.

2.3.2.4 Impact on Market and Transition Challenges

The implementation of the IVDR has posed challenges for stakeholders:

- **Increased Demand on Notified Bodies**: The higher volume of devices requiring assessment has strained the capacity of notified bodies. To address this, the **European Parliament** called for a smooth transition to avoid market disruptions.
- **SMEs**: While the regulation aims to ensure their inclusion, SMEs face significant burdens in adapting to the new requirements, particularly regarding documentation and conformity assessments.
- **Availability of IVD Devices**: Concerns remain about the potential impact on the availability of critical devices due to compliance bottlenecks and transitional complexities.

The IVDR marks a critical step in ensuring the safety, quality, and performance of in vitro diagnostic devices in the EU. By addressing gaps in the previous regulatory framework and aligning with global standards, the IVDR enhances public trust in medical diagnostics while fostering innovation and maintaining a robust market for high-quality devices. Stakeholders must remain vigilant to ensure smooth transitions and sustained market availability.

2.3.3 Guidance on Cybersecurity for Medical Devices (MDCG)

The **Guidance on Cybersecurity for Medical Devices (MDCG 2019-16 Rev.1)** [17], issued in December 2019 by the **MDCG**, was developed to assist manufacturers in complying with the **General Safety and Performance Requirements (GSPRs)** related to cybersecurity as outlined in Annex I of the **MDR** and **IVDR**. Although neither MDR nor IVDR explicitly addresses

Funded by the Horizon Framework Programme of the European Union

cybersecurity, the MDCG guidance provides valuable insights into integrating cybersecurity considerations into medical device design, manufacturing, and post-market processes.

2.3.3.1 Objectives and Scope

The guidance primarily aims to:

- Assist manufacturers in fulfilling cybersecurity-related GSPRs of MDR and IVDR.
- Offer recommendations for other stakeholders in the medical device supply chain, including integrators, operators, and healthcare professionals.
- Bridge the conceptual gap between **safety** and **security**, emphasising their interconnectedness in the context of medical devices.

Despite these objectives, the guidance is **not legally binding**, leaving room for varied interpretations and implementation approaches among stakeholders. This lack of binding authority undermines the harmonisation goals of MDR/IVDR and creates potential inconsistencies in cybersecurity practices.

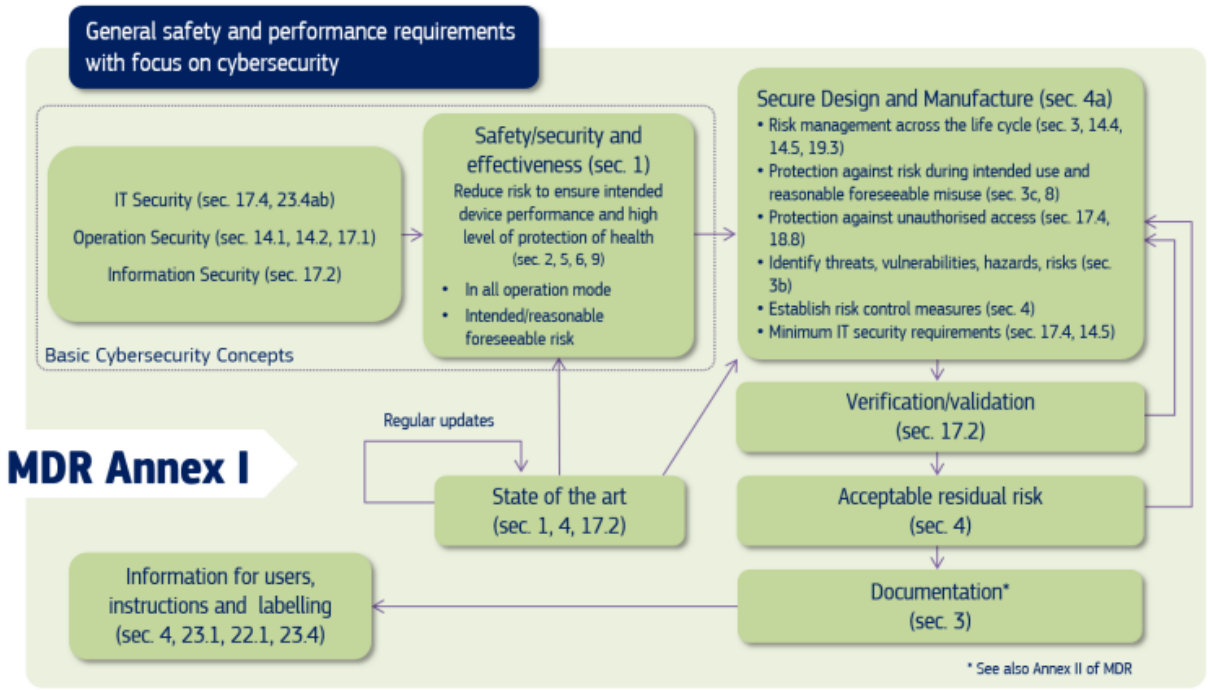

Figure 4: Cybersecurity Requirements Contained in MDR Annex I. Source: MDCG Guidance, p5 [17].

2.3.3.2 Key Provisions

The MDCG guidance addresses cybersecurity from a lifecycle perspective, covering both **pre-market** and **post-market** stages. Its recommendations include the following:

- **Pre-Market Considerations**:
  - **Security by Design**: Encourage embedding cybersecurity measures throughout the design and development phases to ensure robust defences against threats.

Funded by the Horizon Framework Programme of the European Union

- **Risk Management**: Advocate for continuous risk assessment and mitigation, particularly for vulnerabilities in hardware, software, and interfaces.
- **Validation and Verification**: Highlight the importance of rigorous testing to validate the effectiveness of implemented cybersecurity measures.

- **Post-Market Responsibilities**:
  - **Monitoring and Updates**: Recommend post-market surveillance to detect and address emerging threats, including software updates and patches.
  - **Incident Reporting**: Stress the need for mechanisms to report cybersecurity incidents promptly, ensuring minimal impact on patient safety.
- **Shared Responsibilities**:
  - Emphasise collaboration among manufacturers, healthcare providers, regulators, and patients to create a secure ecosystem.
  - Advocate for patient and user awareness about privacy, secure device usage, and recognising suspicious activities.

2.3.3.3 Gaps and Challenges

While the MDCG guidance provides a robust framework for addressing cybersecurity, it also presents several challenges:

- **Terminological Gaps**: The guidance lacks definitions for key terms such as "cybersecurity," "security-by-design," and "security-by-default," which hinders the practical application of its principles.
- **Limited Integration with Other Frameworks**:
  - Although the guidance mentions related regulations such as the **Cybersecurity Act (CSA)**, **GDPR**, and the **NIS Directive**, it does not clarify their interplay with MDR and IVDR, leaving stakeholders to navigate potential overlaps independently.
  - The absence of references to the **Radio Equipment Directive (RED)** [18], which applies to devices with wireless communication capabilities, creates additional ambiguity for manufacturers of CMDs.
- **Dynamic Regulatory Landscape**:
  - The cybersecurity regulatory environment has evolved significantly since the guidance's publication. For instance, the **NIS Directive** mentioned in the guidance has been replaced by the **NIS2 Directive**, which broadens the scope to include medical device manufacturers.

Funded by the Horizon Framework Programme of the European Union

- The guidance does not reflect these updates, making it partially outdated in its recommendations.

- **Ethical Considerations**:
  - Ethical issues, central to cybersecurity practices, are absent from the guidance. Addressing ethical principles would support the implementation of responsible and patient-focused cybersecurity measures.

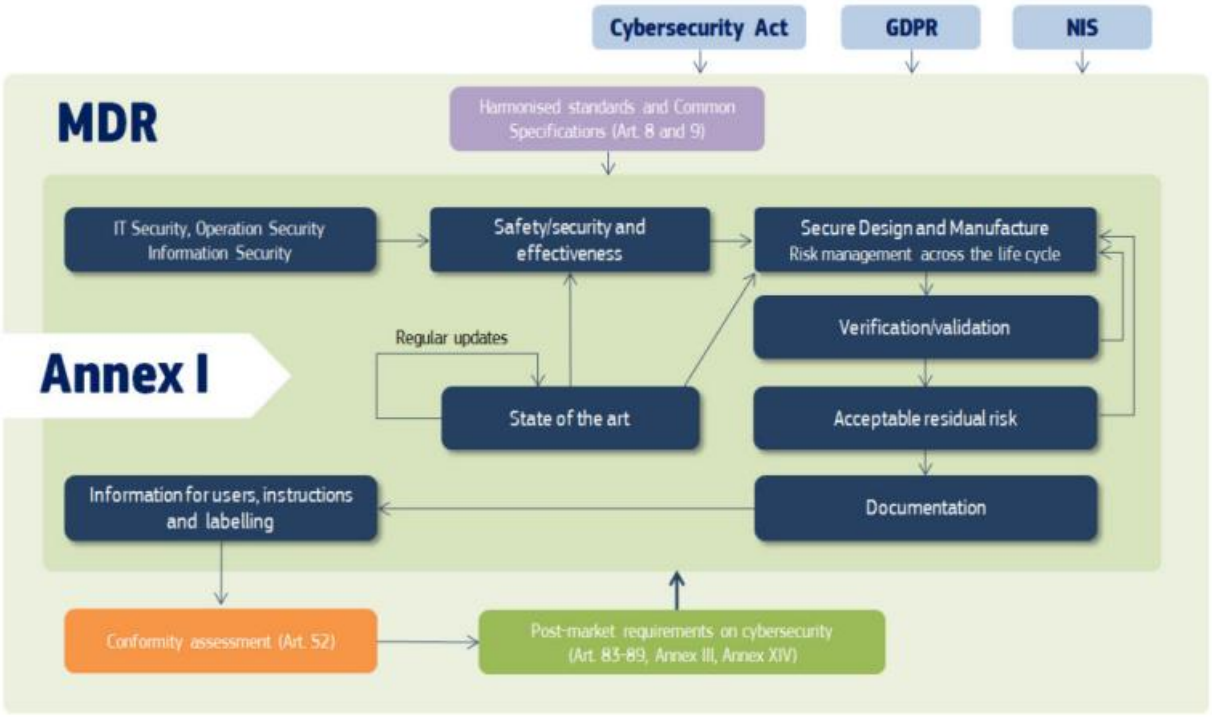

Figure 5: Cybersecurity Requirements in the MDR. Source: MDCG Guidance, p6. [17].

2.3.3.4 Recommendations for Improvement

To enhance its utility and relevance, the MDCG guidance could:

- Include clear definitions and practical examples to bridge theoretical concepts and actionable measures.
- Clarify the interplay between MDR/IVDR and other regulatory frameworks, such as CSA, to reduce inconsistencies and compliance burdens.
- Acknowledge recent regulatory changes, such as the introduction of the NIS2 Directive, to ensure stakeholders are aware of the latest requirements.
- Address ethical considerations to foster trust and accountability in cybersecurity practices.

The MDCG guidance represents a significant step forward in aligning cybersecurity with MDR/IVDR requirements, but its limitations highlight the need for continuous updates and integration with evolving regulatory landscapes. By addressing these gaps, the guidance could

Funded by the Horizon Framework Programme of the European Union

serve as a more comprehensive tool for stakeholders, ultimately enhancing the cybersecurity of medical devices and ensuring patient safety in a rapidly changing digital environment.

2.4 Artificial Intelligence and Ethical Principles

As part of this initiative, ENTRUST introduces AI-driven solutions and components, whose detailed technical design and implementation are analytically discussed in the deliverables D2.1 (Initial Release) and D2.2 (Final Release). These solutions address critical challenges in CMDs, including security, privacy, and real-time risk assessment, leveraging features such as AI-based behavioural analysis and dynamic trust evaluation frameworks. This section focuses on the legal and ethical frameworks relevant to these AI-based solutions, ensuring compliance with EU regulations and ethical principles.

2.4.1 Artificial Intelligence Act (AI Act)

The **Artificial Intelligence Act (AI Act)** [10], formally adopted on **March 13, 2024**, is the world's first comprehensive regulatory framework designed to govern the development, deployment, and use of artificial intelligence. This groundbreaking regulation establishes clear guidelines and obligations for AI developers and deployers while simultaneously promoting innovation and maintaining fundamental human rights and ethical principles. The AI Act is part of the EU's broader strategy to position Europe as a global leader in trustworthy AI, complementing initiatives such as the **AI Innovation Package** and the **Coordinated Plan on AI**.

Though the **AI Act** entered into force on August 1 and will become fully applicable in two years, with certain provisions such as prohibitions taking effect after six months, governance rules and obligations for general-purpose AI models after 12 months, and rules for AI systems embedded into regulated products after 36 months, it is essential for stakeholders, including projects like **ENTRUST**, to anticipate and integrate its requirements. By leveraging initiatives like the **AI Pact**, which encourages voluntary compliance ahead of enforcement, ENTRUST can ensure long-term alignment, sustainability, and a smooth transition to the new regulatory framework.

2.4.1.1 Scope of the AI Act

The AI Act addresses specific risks posed by AI systems while seeking to foster trust among users. Although AI technologies can significantly contribute to solving societal challenges, they also present unique risks, such as bias, opacity, and potential misuse. For instance:

- **Opacity in decision-making**: AI systems often operate as "black boxes," making it difficult to understand or challenge decisions, such as those related to hiring or access to public benefits.
- **Ethical concerns**: Practices like social scoring or biometric surveillance can infringe on privacy and human dignity.

Funded by the Horizon Framework Programme of the European Union

Existing legislation has been insufficient to address these challenges comprehensively, necessitating the development of the AI Act. The regulation establishes a framework that balances **risk mitigation** with **innovation support**, particularly for small and medium-sized enterprises (SMEs).

The AI Act has a broad scope, encompassing both material and territorial dimensions (Article 2). It applies to:

- Providers developing or placing AI systems or general-purpose AI models on the EU market.
- Deployers using AI systems within the Union.
- Providers and deployers located in third countries whose AI system outputs are used in the EU.
- Importers, distributors, and authorised representatives of AI systems.

Notably, the Act excludes areas beyond EU law's scope, such as military and national security, and AI systems developed solely for scientific research (provided fundamental rights and EU laws are respected). However, testing in real-world conditions is not exempt, indicating a likely impact on ENTRUST solutions, which involve both Union-based providers and users.

2.4.1.2 Definitions Under the AI Act

The AI Act introduces critical definitions to clarify obligations:

- **AI System**: A machine-based system designed to operate with varying autonomy, potentially exhibiting adaptiveness post-deployment. It generates outputs like predictions, recommendations, or decisions influencing physical or virtual environments (Article 3(1)(1)).
- **Provider**: Any natural or legal entity developing an AI system or placing it on the market under its own name or trademark, whether for payment or free of charge (Article 3(3)).
- **Deployer**: Any entity using an AI system under its authority, excluding personal non-professional activities (Article 3(4)).

2.4.1.3 Risk-Based Approach

The AI Act adopts a **risk-based approach**, categorising AI systems into four levels:

- **Unacceptable Risk**: Prohibited practices incompatible with fundamental rights (Article 5), such as:
    - Subliminal manipulation.
    - Exploitation of vulnerabilities.
    - Social scoring systems.
    - Real-time biometric identification in public spaces for law enforcement.

Funded by the Horizon Framework Programme of the European Union

- **High Risk**: Systems requiring strict obligations, such as risk mitigation, transparency, and human oversight (Article 6). Examples include AI in critical infrastructure, healthcare, and law enforcement.
- **Limited Risk**: Systems subject to transparency obligations, such as chatbots, ensuring users are informed.
- **Minimal or No Risk**: Systems with negligible risks, such as spam filters, requiring no additional obligations.

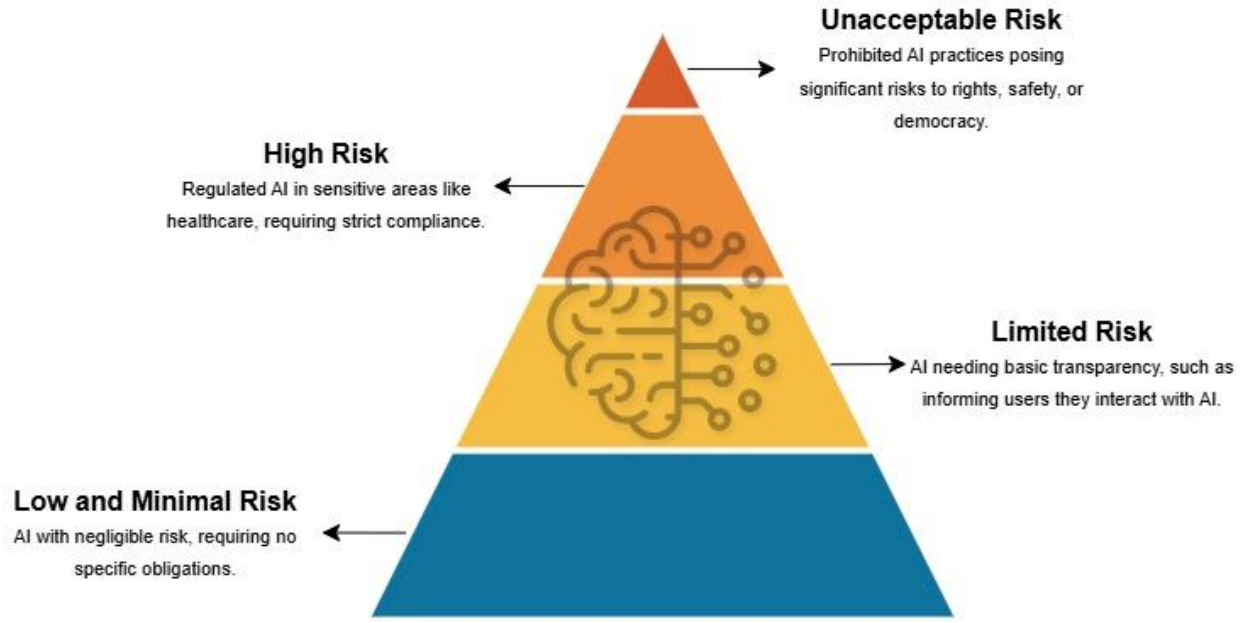

Figure 6: Risk Levels Specified Under the AI Act Proposal. Source: European Commission, 'Regulatory Framework Proposal on Artificial Intelligence' (Shaping Europe's Digital Future) [10].

2.4.1.4 High-Risk AI Systems and Obligations

High-Risk AI Systems

High-risk AI systems, particularly relevant for ENTRUST, must comply with:

- **Risk and quality management systems (Article 9):** Ensures systematic management of risks and quality throughout the AI lifecycle.
- **Data governance and quality requirements (Article 10):** Mandates high-quality, unbiased datasets to minimise risks and discrimination.
- **Detailed technical documentation (Article 11):** Requires comprehensive records to demonstrate compliance and facilitate assessments.
- **Activity logging for traceability (Article 12):** Logs activities to ensure results are traceable and auditable.
- **Transparency measures and human oversight (Articles 13-14):** Ensures clarity in AI operations and human control over critical decisions.

Funded by the Horizon Framework Programme of the European Union

- **Cybersecurity standards for accuracy and robustness (Article 15):** Protects against vulnerabilities and ensures consistent performance.

Deployers of high-risk AI systems also have specific obligations, including:

- **Implementing appropriate technical and organisational measures (Article 26(1)):** Aligns usage with system instructions and safety guidelines.
- **Ensuring human oversight by trained personnel (Article 26(2)):** Assigns responsibility to competent individuals for monitoring AI use.
- **Reporting serious incidents to providers (Article 26(5)):** Requires timely notification of critical issues to the AI system provider.
- **Retaining logs and conducting impact assessments (Articles 26(6) and 26(9)):** Keeps detailed records and assesses potential data protection risks.
- **Informing individuals subject to high-risk AI use (Article 26(11)):** Ensures transparency for affected individuals about AI system interactions.

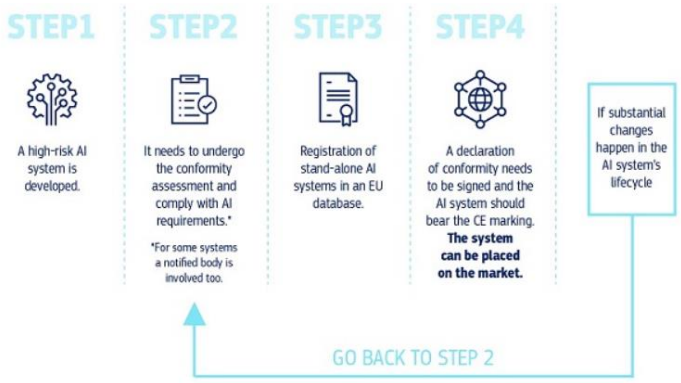

Figure 7: How does it all work in practice for providers of high-risk AI systems? [10]

2.4.1.5 Cybersecurity in the AI Act

Cybersecurity is integral to the AI Act's provisions. Article 15 mandates that high-risk AI systems achieve appropriate levels of accuracy, robustness, and cybersecurity throughout their lifecycle. Measures must address vulnerabilities such as:

- **Data poisoning**: Manipulation of training datasets.
- **Model poisoning**: Compromising pre-trained components.
- **Adversarial examples**: Inputs designed to cause model errors.
- **Confidentiality attacks**: Exploiting system flaws.

Recital 76 underscores the importance of cybersecurity in defending against malicious exploitation of AI vulnerabilities, including attacks targeting training datasets and digital assets. Suitable controls must also account for underlying ICT infrastructure risks.

Funded by the Horizon Framework Programme of the European Union

2.4.1.6 Implications for ENTRUST

The AI Act is particularly relevant to ENTRUST's AI-driven solutions, including those used for behavioural analysis and dynamic trust evaluation in **CMDs**. While these solutions are unlikely to fall under the category of **unacceptable risk**, they may be classified as **high-risk** systems if they function as safety-critical components in CMDs or are subject to conformity assessments under related EU legislation like the **MDR**.

To ensure compliance, ENTRUST:

- Aligns with **risk and quality management standards**.
- Establishes robust **cybersecurity measures** to protect AI models and data.
- Prepares for potential **conformity assessments** if classified as high-risk systems.

2.4.1.7 Transparency and Trustworthiness

In addition to addressing risks, the AI Act promotes transparency by requiring labelling for AI-generated content, such as deepfakes, and informing users when they interact with AI systems like chatbots. These measures aim to build trust and empower users to make informed decisions.

2.4.1.8 Future-Proofing and Governance

The AI Act adopts a future-proof approach, enabling adaptability to evolving technologies. The newly established **European AI Office** oversees enforcement and fosters collaboration among stakeholders. The **AI Pact**, a voluntary initiative, encourages developers to adopt the Act's principles ahead of enforcement to ensure a smoother transition.

The AI Act represents a milestone in the governance of AI technologies, providing a comprehensive framework to balance innovation with ethical considerations. For projects like ENTRUST, early adoption of the Act's provisions ensures compliance, enhances trustworthiness, and strengthens the societal impact of its AI-driven solutions.

2.4.2 Trustworthy AI

On 8 April 2019, the High-Level Expert Group on Artificial Intelligence (AI HLEG) presented the Ethics Guidelines for Trustworthy Artificial Intelligence [19], providing practical guidance for developers, implementers, and users of AI systems. The guidelines aim to ensure that AI systems align with EU fundamental rights and adhere to principles that promote trustworthiness, defined as a prerequisite for the development, deployment, and use of AI.

2.4.2.1 Core Principles of Trustworthy AI

The Guidelines propose that **trustworthy AI** must meet three foundational criteria:

1. **Lawful** – Complying with applicable laws and regulations, including EU and international human rights laws.
2. **Ethical** – Upholding ethical principles and societal values, particularly in areas where legal norms are insufficient.

Funded by the Horizon Framework Programme of the European Union

3. **Robust** – Ensuring both technical and societal robustness to minimise unintended harm and ensure reliability.

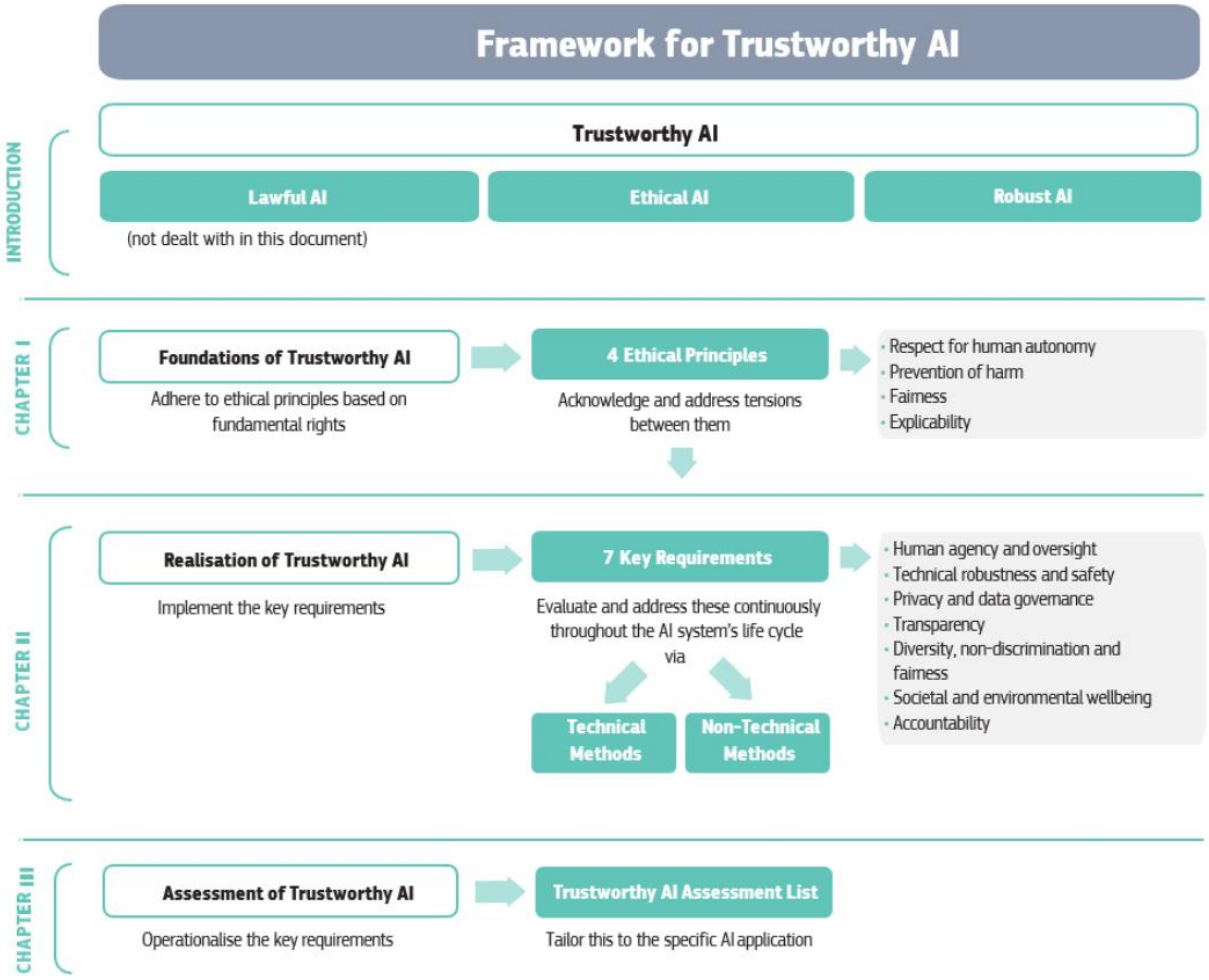

Figure 8: AI High-level expert group Framework for Trustworthy AI. Source: Ethics Guidelines for Trustworthy AI p.10 [19]

2.4.2.2 Seven Key Requirements for Trustworthy AI

To operationalise these principles, the Guidelines identify **seven key requirements**:

- **Human Agency and Oversight**
  - AI systems must empower individuals, allowing informed decision-making while respecting fundamental rights.
  - Oversight mechanisms include approaches like **human-in-the-loop**, **human-on-the-loop**, and **human-in-command** to ensure appropriate control.
- **Technical Robustness and Safety**
  - AI systems must be **secure, reliable, and resilient**, with safeguards like fallback mechanisms to handle failures.

Funded by the Horizon Framework Programme of the European Union

- Measures should address **security risks** such as data poisoning, adversarial attacks, and unintended dual-use scenarios.

- **Privacy and Data Governance**
  - Systems must respect privacy and comply with **data protection laws**, ensuring data quality, integrity, and transparency in access protocols.
- **Transparency**
  - AI processes, models, and decisions should be traceable and explainable to relevant stakeholders.
  - Users must be informed when interacting with AI and should understand its capabilities and limitations.
- **Diversity, Non-discrimination, and Fairness**
  - AI systems must avoid biases that could lead to discrimination or marginalisation.
  - Accessibility and inclusivity should be prioritised, involving stakeholders throughout the AI system lifecycle.
- **Societal and Environmental Well-being**
  - AI systems must promote **sustainability** and consider their impact on the environment and society, benefiting present and future generations.
- **Accountability**
  - Clear mechanisms must ensure accountability for AI outcomes, including **audibility**, impact assessments, and accessible redress systems.

2.4.2.3 Ethical Principles for AI

The Guidelines are grounded in **four ethical principles**, based on EU fundamental rights:

1. **Respect for Human Autonomy** – Ensures AI does not unjustly manipulate or coerce individuals and promotes human-centric design.
2. **Prevention of Harm** – Requires robust security measures to mitigate potential risks and adverse impacts.
3. **Fairness** – Demands equitable outcomes, avoiding biased decisions that harm vulnerable groups.
4. **Explicability** – Promotes transparency and understanding of AI processes, enabling trust and accountability.

Funded by the Horizon Framework Programme of the European Union

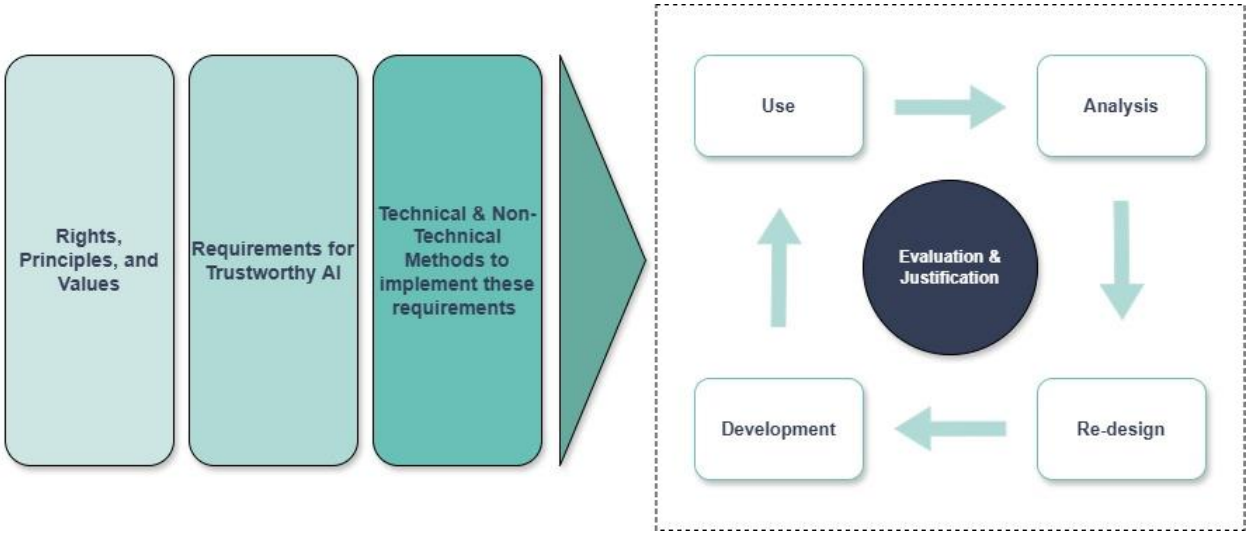

Figure 9: Trustworthy AI Life Cycle. Source: Ethics Guidelines for Trustworthy AI p.20 [19].

2.4.2.4 Operationalising Trustworthy AI

The **Assessment List for Trustworthy Artificial Intelligence (ALTAI)** [20] provides a practical self-assessment tool for developers and deployers to evaluate adherence to the seven requirements. Key operational methods include:

- **Technical measures** such as X-by-design approaches, explanation methods (e.g., XAI), and validation tools.
- **Non-technical measures** like standardisation, codes of conduct, and certification mechanisms.

The Ethics Guidelines also highlight the importance of continuous monitoring and improvement across the AI system lifecycle to ensure long-term adherence to ethical principles.

2.4.2.5 Implications for ENTRUST

For ENTRUST, which integrates AI-driven solutions into **CMDs**, these guidelines serve as a benchmark for developing trustworthy AI that respects privacy, ensures transparency, and fosters inclusivity. By adopting the Ethics Guidelines:

- ENTRUST can strengthen its commitment to **human-centric AI design**.
- It ensures compliance with ethical standards that complement legal obligations, such as those under the AI Act.
- The project contributes to societal and environmental well-being while maintaining accountability through clear governance structures.

To further bolster the credibility and ethical integrity of the ENTRUST project, all activities involving AI will be analysed following the HUDERIA methodology, officially adopted by the Council of Europe Committee on Artificial Intelligence on 28 November 2024. This methodology, aligned with the AI Act requirements for Fundamental Rights Impact Assessments (FRIAs),

Funded by the Horizon Framework Programme of the European Union

provides a structured framework for evaluating AI systems' impact on fundamental rights. By employing HUDERIA, ENTRUST ensures a rigorous assessment of its AI-driven solutions, reinforcing trust and societal acceptance through adherence to best practices.

2.5 Clinical Research and Ethical Practices

2.5.1 Objectives and Challenges in Clinical Research

The primary goal of clinical research is to produce generalisable knowledge to improve health and deepen understanding of human biology. This field is especially challenging when involving vulnerable groups such as children and young people, as ethical and practical concerns arise due to their unique needs and developmental stages. Ensuring their safety requires robust protections to prevent exploitation, while recognising the necessity of research for understanding and treating childhood diseases.

2.5.2 Emerging Technologies in Clinical Research

Advances in **digital devices**, **data analytics**, and **artificial intelligence** are transforming clinical research. Tools like **remote monitoring technologies (RMTs)**—including wearables, smartphone apps, and home-based sensors—allow real-time, continuous, and objective data collection. These innovations provide deeper insights into health behaviours and outcomes but also introduce critical ethical challenges, particularly regarding **privacy** and **data security**.

2.5.3 Ethical Frameworks and Guidelines

Ethical standards in clinical research are shaped by foundational international instruments that provide a robust framework to safeguard participants' rights, ensure ethical conduct, and maintain scientific integrity. These include:

- **Universal Declaration of Human Rights (UDHR)**: Adopted by the United Nations in 1948, the UDHR underscores the inherent dignity and equal rights of all individuals. It lays the foundation for ethical research practices by emphasising the rights to life, liberty, privacy, and freedom from discrimination.
- **European Convention on Human Rights (ECHR):** This legally binding treaty focuses on protecting civil and political rights. In clinical research, it underlines the importance of privacy, informed consent, and the right to freedom from harm and exploitation.
- **Declaration of Helsinki**: Created by the World Medical Association, this cornerstone document outlines ethical principles for medical research involving human subjects. It prioritises informed consent, the need for scientifically sound research designs, and the welfare of participants, especially vulnerable populations.
- **ICH Guidelines on Good Clinical Practice (E6 and E11):** These international standards ensure the ethical and scientific quality of clinical trials, focusing on participant rights, safety, and robust documentation. They also address the specific challenges of

Funded by the Horizon Framework Programme of the European Union

conducting clinical research involving paediatric populations, such as obtaining informed assent and parental consent.

- **CIOMS International Ethical Guidelines**: Issued by the Council for International Organizations of Medical Sciences, these guidelines focus on ethical review processes, informed consent, and the protection of vulnerable populations, particularly children. They provide practical recommendations for conducting ethically responsible health-related research.

With the integration of **AI** and **remote monitoring technologies**, ethical concerns expand to include:

- Safeguarding **privacy and confidentiality** of sensitive health data.
- Ensuring **informed consent** is adapted to the complexities of digital data collection.
- Addressing potential biases in AI systems to prevent discrimination.

The **Declaration of Helsinki** and **ICH-GCP guidelines** remain pivotal for ensuring ethical standards in clinical trials, particularly regarding:

- Transparency in protocols and participant communication.
- Independent ethical oversight.
- Comprehensive data governance measures.

Additionally, the **Clinical Trials Regulation (CTR)** standardises trial procedures across the EU, enhancing efficiency while prioritising participant safety.

All these frameworks outline fundamental principles and practices to protect research participants, emphasising respect for human rights, autonomy, and informed consent.

2.5.4 Informed Consent, Assent, and Dissent

Informed consent is the cornerstone of ethical clinical research, ensuring participants fully understand the nature, risks, and benefits of a study before voluntarily agreeing to participate. In paediatric research, **assent** (a child's affirmative agreement) and **dissent** (refusal to participate) are critical, reflecting children's evolving capacities to understand and make decisions.

2.5.5 Principles of Biomedical Ethics

Four cardinal principles guide ethical biomedical research:

1. **Autonomy**: Respecting participants' rights to make informed decisions.
2. **Non-maleficence**: Avoiding harm to participants.
3. **Beneficence**: Maximising benefits while minimising harm.
4. **Justice**: Ensuring fair selection and treatment of participants.

Although there is no direct requirement for ENTRUST to adhere to all the ethical frameworks mentioned above, the consortium has consciously integrated these principles into its operations.

Funded by the Horizon Framework Programme of the European Union

By going beyond compliance, ENTRUST aims to produce long-term results that not only benefit stakeholders during the project lifetime but also establish a lasting impact on ethical, secure, and innovative healthcare solutions.

2.6 Ethics

2.6.1 Competent bodies and requirements in ENTRUST project

The internal, ethical compliance of the project is monitored by the Ethics Manager, the Ethics Committee the Project Security Board and WP1, Project Management in terms of T1.4.

2.6.1.1 Ethics Manager

As part of the ENTRUST project, Ms. Anna Palaiologk has been appointed as the Ethics Manager, a role crucial to ensuring the project adheres to the highest standards of ethical oversight. With extensive experience in the ethical monitoring of research initiatives, Ms. Palaiologk plays an important role in overseeing compliance processes and reviewing related documentation.

2.6.1.2 Ethics Committee

The ENTRUST Ethics Committee (EC) was established in M03 of the project, as outlined in the Project Handbook (D1.1), where it is referred to as the Legal & Ethics Monitoring Team. Its formation is of critical importance due to the complex and challenging ethical issues inherent in the project, particularly concerning the development and deployment of Trust Assessment Framework and other components related to CMDs. The EC is composed of interdisciplinary experts from fields such as medical science, law, data protection, research ethics, and engineering, and is guided by a policy expert and an ethicist.

The Ethics Manager (EM), Ms. Anna Palaiologk, chairs the Ethics Committee, working in collaboration with the Project Coordinator (PC), the Research Manager (RM), and Work Package (WP) leaders. Together, they ensure that ethical compliance is maintained across all project activities, aligning with EU regulations and the ENTRUST legal and ethical guidelines.

Given the sensitive nature of the ENTRUST project, which involves personal health data, patient safety, and trust management, the Ethics Committee plays a pivotal role in addressing potential ethical issues. The committee's responsibilities include:

- Providing all partners with ethical guidelines for conducting research, performing tasks, or engaging in project activities.
- Ensuring that all consortium partners adhere to the relevant legal frameworks.
- Overseeing the ethical treatment and safeguarding of all data collected and processed during the project.
- Maintaining the ethical dimension across ENTRUST activities.
- Guaranteeing that dissemination and exploitation activities respect privacy and do not compromise the rights of any actor or entity involved in the project.

Funded by the Horizon Framework Programme of the European Union

- Managing incidents or incidental findings during the research process, ensuring an ethical resolution.
- Reviewing all study-related materials and methodologies before and during the project.
- Performing periodic reviews to ensure continuous monitoring of ethical compliance throughout the project's lifecycle.

The research conducted within ENTRUST is held to the highest standards of rigor and integrity. The Project Coordinator, supported by Consortium Members and the Ethics Committee, ensures full compliance with EU regulations and ethical guidelines. The Legal & Ethics Monitoring Team, underscores the consortium's commitment to maintaining high ethical standards across academic, industrial, research, and stakeholder engagement activities.

2.6.2 Ethical Issues in CMDs

In addition to the legal aspects, the **ethical dimension** of CMDs is paramount, as these devices collect and transmit sensitive personal health data. Patients must be assured that their data is secure, private, and used exclusively for their benefit. Based on the project analysis, the following key ethical issues are considered:

1. **Informed Consent for Data Use**: Users must be **fully informed** about how their data will be collected, stored, and used. This includes transparent communication about the purpose of the data collection, ensuring that consent is truly informed and voluntary.
2. **Safety and Transparency**: Users need confidence that the devices are **safe, reliable**, and meet the required standards for usage. They must also be informed of any potential risks, ensuring transparency at every stage of deployment and operation.
3. **Post-Update and Integration Safety**: Devices must remain safe and effective after updates or when integrated into different clinical settings. Transparent communication about changes and potential risks post-update is essential to maintain trust and safety.
4. **Consent for Research Use of Data**: Explicit consent must be obtained for the use of personal data in research. Patients should retain the right to access and control their data, ensuring ethical usage beyond clinical applications.
5. **Informational Privacy**: Patients have a fundamental right to **privacy and confidentiality**. Data must not be shared or sold without explicit patient consent, safeguarding against misuse and ensuring compliance with privacy regulations.
6. **Ownership and Data Access:** Patients must be clearly informed about **data storage locations** and **access permissions**, including the identities of parties with authorised access to their data. This ensures transparency and aligns with ethical data ownership principles.

Funded by the Horizon Framework Programme of the European Union

7. **Trustchain Preservation and Ethical Responsibilities to Stakeholders**: A trustchain that encompasses all stakeholders must be preserved, ensuring that ethical standards are consistently upheld throughout the data lifecycle. This includes providing visible and verifiable certifications, such as the **GDPR Art. 42 certification**, which reassures data subjects of the compliance and accountability of systems and processes. By maintaining the integrity of the trustchain, ENTRUST ensures transparency, ethical accountability, and sustained trust among all parties, including patients, providers, and regulators.

2.6.3 Ethical Applications in ENTRUST Use Cases

The ENTRUST project integrates these ethical considerations into its **Trust Assessment Framework** and use cases to ensure compliance and demonstrate commitment to ethical excellence:

- **Ambient Intelligent System for Independent Living**
  - Security is enhanced using **Verifiable Credentials** and **Blockchain auditability** to ensure privacy and data integrity across hierarchical systems.
  - Patients are assured that their data is used solely for their benefit while maintaining safety and transparency in operations.
- **Digital Assistance for Patient Health and Well-being**
  - ENTRUST ensures secure data exchange between ambulances and hospitals, minimising vulnerabilities in CMD networks.
  - Safety and transparency are prioritised in integrating CMDs into hospital IT infrastructures while addressing legal and ethical concerns.
- **Wearable Devices for Mental Health Monitoring**
  - ENTRUST's framework ensures **data integrity** and privacy during wearable-to-mobile communications.
  - Devices are regularly assessed to ensure **operational safety and effectiveness** throughout their lifecycle, including updates and research applications.

2.7 Other Standard, Legal and Ethical Issues Relevant to ENTRUST

The ENTRUST project operates in a complex landscape of legal, ethical, and standardisation frameworks to ensure compliance and promote best practices. Several standards, conventions, and guidelines are directly relevant to the project, shaping its approach to data protection, cybersecurity, and the ethical use of technology in healthcare.

Funded by the Horizon Framework Programme of the European Union

2.7.1 Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108)

Established by the Council of Europe, Convention 108 is the first and only legally binding international treaty [21] guaranteeing the right to data protection. It enshrines principles such as lawfulness, purpose limitation, and data quality, ensuring secure and lawful processing of personal data. For ENTRUST, which involves collecting and processing sensitive health data through CMDs, adherence to Convention 108 safeguards patient rights and reinforces trust in data management practices.

2.7.2 Council of Europe Convention on Cybercrime (Budapest Convention)

The Budapest Convention serves as a comprehensive framework to combat cybercrime, focusing on harmonising national laws, improving investigative techniques, and fostering international cooperation. For ENTRUST, which relies on secure communication in CMD, the Convention ensures robust protection against cyberattacks targeting sensitive patient data and critical healthcare infrastructure.

2.7.3 Declaration on Research Assessment (DORA)

The Declaration on Research Assessment (DORA) [22] advocates for qualitative evaluation of research outputs, moving beyond metrics like journal impact factors. ENTRUST aligns with DORA principles by emphasising transparency, fairness, and inclusivity in evaluating research contributions, ensuring that project outputs are assessed on their quality and societal impact.

2.7.4 Directive 2002/58/EC (ePrivacy Directive)

The ePrivacy Directive (EU 2002/58/EC) [23] complements the GDPR by addressing privacy and data protection in electronic communications. It establishes rules to ensure confidentiality in online communication, regulate the use of cookies, and require user consent for online tracking activities. For ENTRUST, which involves CMDs transmitting data over electronic networks, adherence to the ePrivacy Directive ensures that the communication infrastructure respects user privacy, secures sensitive information, and fosters trust in the project's technological solutions.

2.7.5 IEC 62304

The IEC 62304 standard specifies lifecycle requirements for the safe design and maintenance of medical device software. It ensures rigorous development processes, mitigating risks associated with software malfunctions. ENTRUST integrates this standard to validate the reliability and safety of its CMD solutions, particularly in their software components.

2.7.6 IEC 81001-5-1

The IEC 81001-5-1 standard provides comprehensive guidelines for the security and safety of health IT systems and software. It addresses interoperability and resilience against cyber threats,

Funded by the Horizon Framework Programme of the European Union

critical for ENTRUST's CMDs. This standard ensures that ENTRUST solutions remain secure, reliable, and compliant with modern healthcare needs.

2.7.7 International Medical Informatics Association (IMIA) Code of Ethics for Health Information Professionals

The IMIA Code of Ethics outlines principles for managing health information ethically, including privacy, confidentiality, and integrity. For ENTRUST, this framework guides the ethical handling of sensitive health data, ensuring alignment with best practices in data management and professional responsibility.

2.7.8 ISO 13606-1:2019 - International Standardization Organization Standards for Electronic Health Records (EHRs)

The ISO 13606-1:2019 standard specifies structures for the secure and interoperable exchange of electronic health records. ENTRUST incorporates this standard to guarantee that patient data remains consistent and secure across heterogeneous systems, enabling seamless data integration in CMDs.

2.7.9 World Health Organization (WHO) Resolution on e-Health

The WHO Resolution on e-Health highlights the transformative role of digital health technologies in enhancing healthcare delivery globally. It encourages responsible adoption of e-health solutions, directly supporting ENTRUST’s mission to leverage advanced technologies like CMDs for improved patient outcomes and health system efficiency.

By adhering to these diverse standards, conventions, and ethical frameworks, ENTRUST ensures a robust and compliant foundation for its activities, further strengthening trust and societal acceptance of its outcomes.

3 Societal Dimensions

3.1 ENTRUST Workshop on Legal and Ethical Issues and Guidelines

The increasing reliance on CMDs in healthcare introduces complex challenges related to data security, privacy, and trust. These challenges are compounded by evolving regulations such as GDPR, MDR, and cybersecurity directives, as well as the growing need to address societal and ethical concerns. Ensuring that CMDs are both legally compliant and ethically trustworthy is essential to their successful integration into healthcare systems.

The Legal and Ethical Dimensions Workshop was organised to support the project's mission of ensuring robust compliance and trust management in CMDs. This workshop focused on gathering inputs from stakeholders to identify and address the ethical and legal challenges associated with the development, deployment, and operation of Trust Framework in CMDs among other topics such as the development of medical devices. By leveraging a combination of systems engineering

Funded by the Horizon Framework Programme of the European Union

and design thinking approach, the workshop aimed to provide a structured pathway to integrate legal compliance and ethical considerations into all phases of definition, development, integration and validation.

This workshop brought together 15 participants from the ENTRUST consortium, representing a diverse range of expertise to foster an interdisciplinary approach and capture multiple perspectives on the ethical and legal challenges surrounding CMDs.

The participants included developers, researchers, legal experts, ethical advisors, and end-users, ensuring that discussions addressed the technical, regulatory, and societal dimensions of CMDs. The diversity of expertise is illustrated in Figure 10Figure 10: Distribution of Participants by Expertise., which highlights the broad spectrum of skills and perspectives represented during the session.

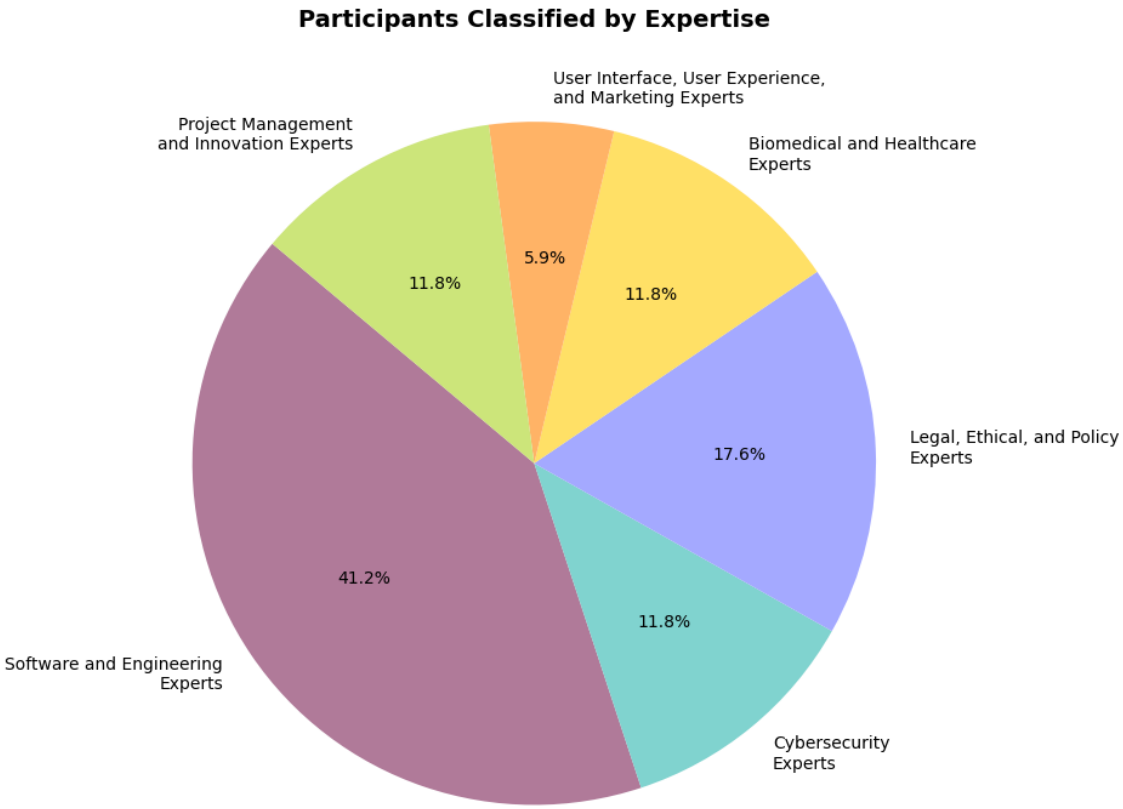

Figure 10: Distribution of Participants by Expertise.

The primary objectives of the workshop were:

- Identify Ethical and Legal Dimensions: To collect insights on the ethical principles and legal standards governing CMDs, focusing on aspects such as data protection, cybersecurity, transparency, and societal trust.
- Evaluate Current Practices and Gaps: To analyse existing compliance practices and identify gaps in addressing ethical and legal requirements across stakeholders' processes.

Funded by the Horizon Framework Programme of the European Union

- Engage Stakeholders Across Disciplines: To facilitate a collaborative discussion involving developers, researchers, end-users, and legal/ethical organisations, ensuring a comprehensive understanding of the challenges.
- Provide the Foundation for a Compliance Methodology: To gather actionable inputs that can be used to develop a dynamic framework addressing legal and ethical challenges while promoting trust in CMDs.

3.1.1 Methodology

The workshop methodology was designed to engage partners in an interactive and collaborative process, enabling them to contribute their expertise to the identification, classification, and analysis of legal and ethical dimensions relevant to CMDs. The methodology leveraged both prior knowledge from ENTRUST activities and deliverables, as well as real-time insights generated during the session.

Participants were informed about the current status of the project and provided with a concise introduction to regulatory frameworks and ethical considerations in CMDs. Most participants already had foundational knowledge from previous ENTRUST activities and deliverables, ensuring a solid baseline for effective engagement. A collaborative workspace was set up to facilitate real-time contributions and simultaneous input during the session.

The workshop comprised four key activities, each aimed at systematically gathering, organising, and analysing inputs from the participants:

- Activity 1: Identification of Legal and Ethical Dimensions
  - Participants were presented with categories such as EU Regulations, National Regulations, Ethical Standards, and Industry-Specific Guidelines.
  - They were tasked with adding relevant keywords, standards, and regulations based on their expertise and experience.
- Activity 2: Classification into a Quadrant (Square Box)
  - Inputs from Activity 1 were classified based on Ethical Sensitivity and Intensity of Legal Impact.
  - The classifications included the following categories:
    - Critical Management: High Ethical Sensitivity, High Legal Impact
    - Ethical Prioritisation: High Ethical Sensitivity, Low Legal Impact
    - Legal Compliance: Low Ethical Sensitivity, High Legal Impact
    - Routine Monitoring: Low Ethical Sensitivity, Low Legal Impact
- Activity 3: Classification into Levels of Attention
  - Participants further categorised inputs into levels reflecting the attention required:
    - Core Compliance: Essential dimensions requiring continuous management.

Funded by the Horizon Framework Programme of the European Union

- Active Management: Dimensions needing periodic oversight and updates.
- General Awareness: Dimensions requiring monitoring but minimal active management.

- Activity 4: Gap Analysis and ENTRUST Strengths
  - Participants provided insights into challenges and gaps in ethical and legal compliance for CMDs, reflecting on their current work and experience.
  - They shared comments on:
    - Gap Analysis: Identifying areas needing improvement and highlighting barriers to compliance or trustworthiness.
    - ENTRUST Strengths: Emphasising the project's achievements in addressing legal and ethical dimensions, based on their involvement and overall project perspective.

Through these sessions participants contributed with insights simultaneously and dynamically. The methodology ensured diverse inputs and promoted interdisciplinary discussions. The activities helped organise the inputs into actionable categories, forming the basis for further analysis.

3.1.2 Workshop Results

The workshop methodology enabled a collaborative and dynamic analysis of the legal and ethical dimensions of CMDs by engaging participants with varied expertise.

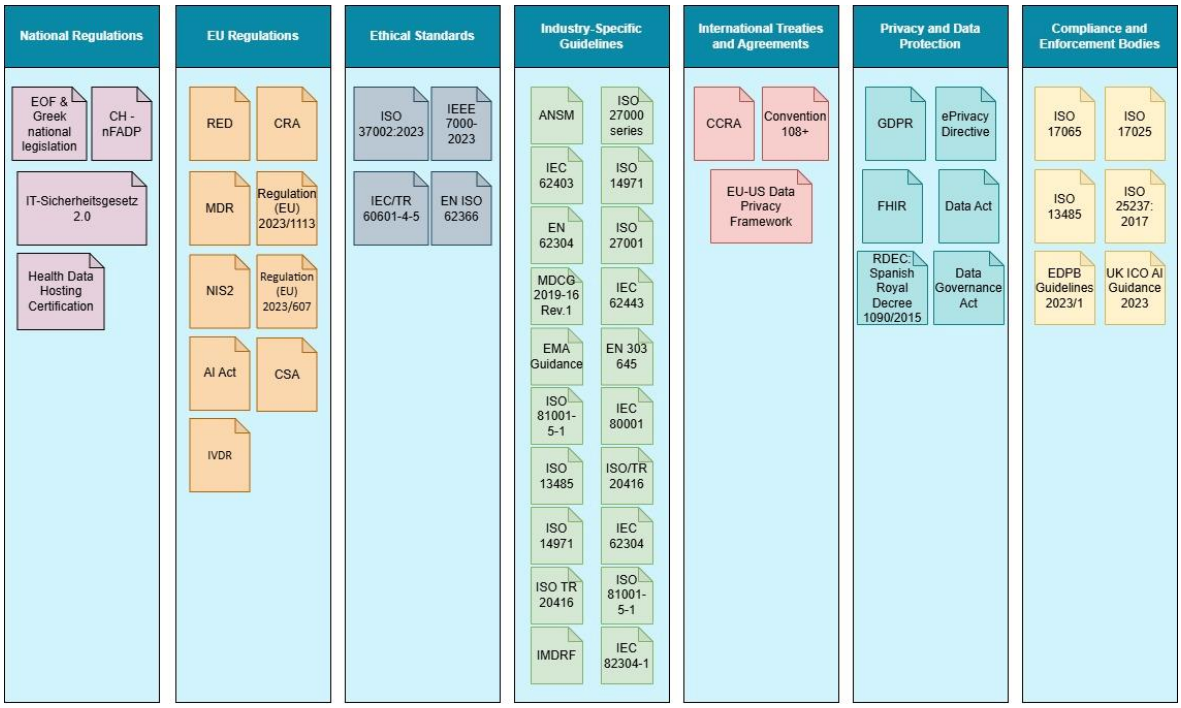

Figure 11: Activity 1: Identification of Legal and Ethical Dimensions

Funded by the Horizon Framework Programme of the European Union

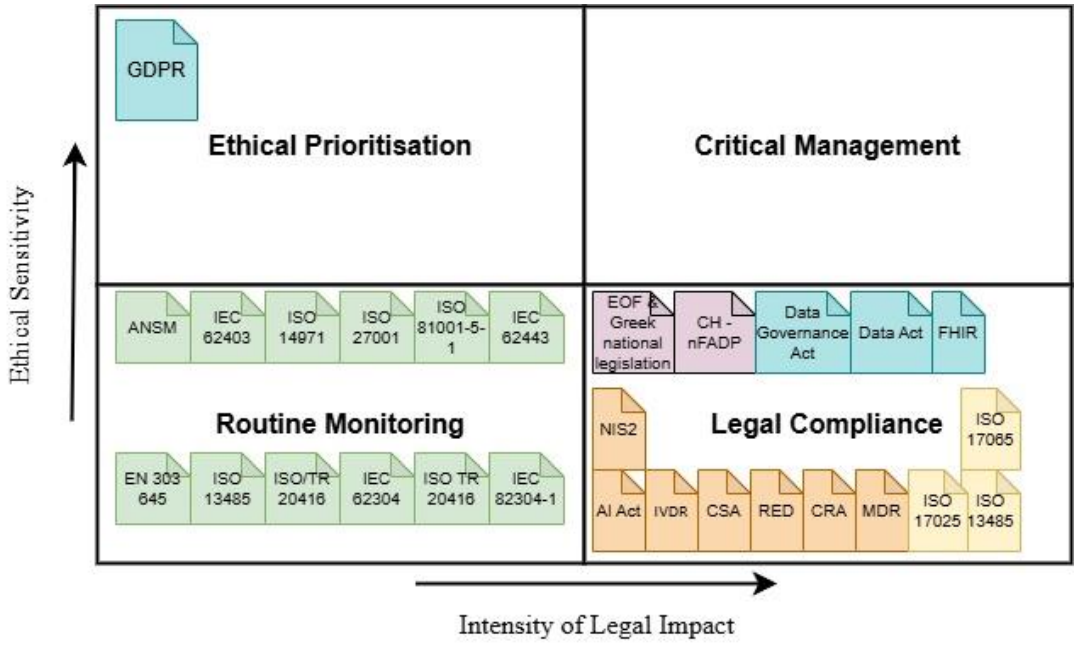

Figure 12: Activity 2: Classification into a Quadrant

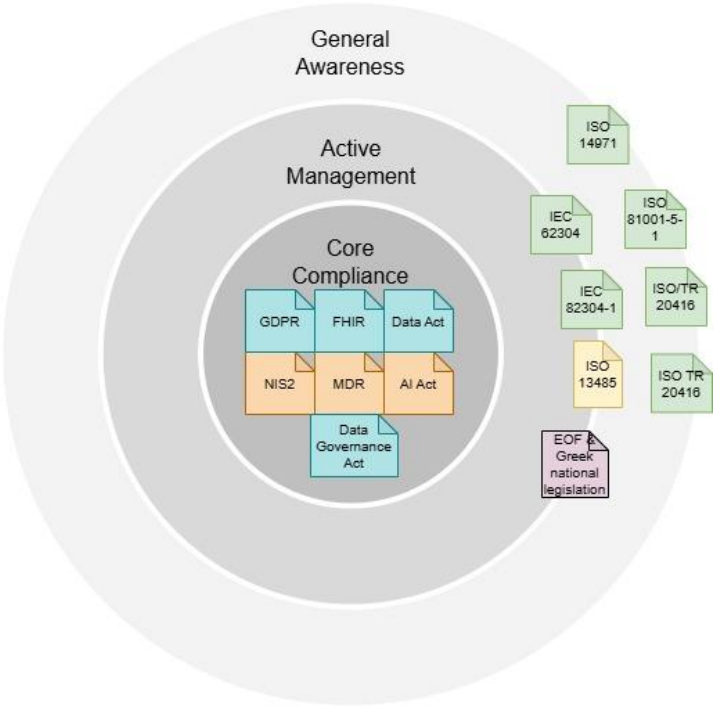

Figure 13: Classification into Levels of Attention

3.2 Public attitudes towards cybersecurity

Public attitudes towards cybersecurity reflect a complex interplay of awareness, trust, risk perception, and behavioural responses. While digital interconnectivity continues to grow, many individuals fail to adopt even basic cybersecurity measures, leaving them vulnerable to cyber

Funded by the Horizon Framework Programme of the European Union

threats. Understanding public perceptions is critical for designing effective policies and interventions, particularly in sectors like healthcare and medical devices, where the stakes are high [24].

3.2.1 Cybersecurity in Healthcare and Medical Devices

Healthcare is often perceived as one of the most trusted sectors for data management. However, this trust can erode rapidly in the wake of incidents such as ransomware attacks or breaches of patient records. The WannaCry attack, which disrupted healthcare services worldwide, is a stark example, amplifying public concerns about the vulnerability of healthcare systems to cyberattacks [25]. For CMDs, these concerns become deeply personal, as they deal directly with individual health and safety. Studies indicate that patients worry about unauthorised access to sensitive health data or device malfunctions caused by cyberattacks [25], [26], [27]. However, the general public often lacks a nuanced understanding of cybersecurity as it pertains to CMDs, frequently assigning the responsibility for data safety to manufacturers and healthcare providers.

3.2.2 Socio-Demographic Determinants and Trust

Empirical studies show that public perceptions of cybersecurity are influenced by socio-demographic factors, trust, and the specific context in which security measures are applied. Trust in institutions—whether public or private—is a key determinant of acceptance. Citizens tend to place greater trust in public sector actors over private entities for managing personal data. However, this trust is contingent on the perceived accountability, transparency, and proportionality of the measures. Transparency plays a pivotal role: citizens are more likely to accept security practices when they understand the necessity and effectiveness of the measures and feel they have been communicated responsibly. For instance, public reactions can vary depending on the context. Security measures perceived as protecting legitimate public interests, such as preventing violent incidents, are generally more accepted than those seen as infringing on fundamental rights like the right to protest. These nuances highlight the importance of clearly communicating the purpose of cybersecurity measures to align them with public expectations.

3.2.3 Clinicians and Expert Users' Perspectives on Cybersecurity

Clinicians and expert users, including biomedical engineers, IT administrators, and healthcare technologists, form a critical stakeholder group in managing cybersecurity for CMDs. Both groups recognise the transformative potential of CMDs in enhancing patient care and operational efficiency but express shared concerns about cybersecurity vulnerabilities, particularly in life-critical systems such as infusion pumps, pacemakers, and hospital networks. This stakeholder group highlights the trade-off between usability and security, where overly complex cybersecurity protocols can hinder timely care delivery and device functionality [28], [29], [30]. Seamless integration of cybersecurity measures into existing workflows is paramount to prevent these measures from inadvertently compromising patient outcomes. Both clinicians and expert users

Funded by the Horizon Framework Programme of the European Union

advocate for transparent, user-friendly cybersecurity frameworks that ensure protection without adding undue burden on end-users. From a technical standpoint, expert users stress the importance of end-to-end security solutions that encompass the entire lifecycle of medical devices, from development to deployment and eventual decommissioning. Compliance with international standards like IEC 62304 and ISO 13485 is considered essential to maintaining robust security. Similarly, clinicians emphasise the need for enhanced training and awareness programs to address human errors, which often contribute significantly to breaches. Both clinicians and expert users value interoperability and auditability in cybersecurity frameworks. Interoperability ensures that CMDs from different manufacturers can integrate seamlessly within broader healthcare IT ecosystems, while auditability facilitates transparent monitoring and assessment of device security and functionality. Dynamic trust management solutions, such as those proposed by ENTRUST, are viewed as pivotal by this stakeholder group for adapting to emerging threats and maintaining confidence in CMDs.

3.2.4 Bridging Public and Expert Perspectives

Public attitudes often contrast with the more technical concerns of clinicians and expert users. While the general public focuses on data privacy and accountability, expert users delve into the intricacies of interoperability, compliance, and lifecycle security. Transparency and trust-building measures can bridge these gaps. Responsible communication about the purpose, effectiveness, and proportionality of cybersecurity measures can align public and expert expectations, fostering a cohesive approach to enhancing the security and trustworthiness of healthcare systems and CMDs. By addressing these diverse perspectives, ENTRUST can design adaptive and transparent cybersecurity frameworks that protect privacy, ensure safety, and maintain trust across all stakeholders.

3.2.5 End-User & Citizens Feedback on Medical Device Trustworthiness

The trustworthiness of medical devices, particularly concerning cybersecurity in healthcare, is a key focus of the ENTRUST project. Understanding how different stakeholder groups perceive the reliability, safety, and security of CMDs is critical for designing effective and acceptable solutions. To achieve this, a targeted questionnaire was developed and distributed to gather insights into public attitudes and the opinions of end-users, including clinicians and technical experts, on medical device trustworthiness and cybersecurity challenges.

3.2.5.1 Target Groups

The target group for the ENTRUST project's feedback collection on CMD trustworthiness and cybersecurity included a comprehensive range of professionals and end-users directly involved with CMDs. These were:

1. **Clinicians, Healthcare Professionals, and Expert Users**: This combined group encompassed physicians, nurses, biomedical engineers, IT administrators, and

Funded by the Horizon Framework Programme of the European Union

healthcare technologists. These individuals play a critical role in the operational, clinical, and technical aspects of CMDs, spanning daily patient care to the implementation, maintenance, and cybersecurity of these devices.

2. **Citizens and Patients**: Individuals who either directly use CMDs or depend on healthcare services supported by CMD-generated data. This group represents the public's perceptions and concerns regarding data privacy, security, and device trustworthiness.

By targeting this mix of clinical, technical, and public stakeholders, the ENTRUST project ensured that diverse insights were captured, addressing both practical and experiential dimensions of CMD usage and trustworthiness.

3.2.5.2 Methodology

To ensure comprehensive feedback from diverse target groups, the ENTRUST project employed a two-questionnaire approach, tailored to each group's unique experiences and perspectives:

3.2.5.2.1 For End Users – Technology Users

A dedicated questionnaire, titled *"Ethical and Legal Considerations in Connected Medical Devices: Feedback from Technology Users,"* was designed to gather insights from clinicians, biomedical engineers, IT administrators, and other healthcare professionals directly engaged with CMDs. This group provided valuable feedback on the operational, usability, and security dimensions of CMDs, reflecting their hands-on experience with these devices.

The questionnaire explored:

- **Usability**: Ease of navigation, accessibility, and clarity of instructions for CMDs.
- **Data Security**: Confidence in data protection mechanisms and cybersecurity standards.
- **Transparency**: Awareness of how personal health data is utilised.
- **Trust and Privacy**: Perspectives on CMD reliability, privacy mechanisms, and trustworthiness.
- **Improvements**: Open-ended responses sought suggestions for enhancing usability and addressing privacy concerns.

3.2.5.2.2 For Citizens – Patients

A separate questionnaire, titled *"Perspectives on Transparency, Security, and Trust in Connected Medical Devices,"* was developed for external stakeholders such as patients and the general public. This questionnaire focused on the end-user perspective regarding transparency, data protection, and ethical practices in CMDs.

The questionnaire examined:

- **Transparency**: Understanding the purpose, functionality, and data usage of CMDs.
- **Security and Privacy**: Perceptions of CMDs' ability to safeguard sensitive health data.

Funded by the Horizon Framework Programme of the European Union

- **Trust and Compliance**: Confidence in CMDs adhering to legal, ethical, and safety standards.
- **Suggestions**: Open-ended questions invited feedback on improving CMD trustworthiness and ethical considerations.

3.2.5.2.3 Distribution and Analysis

- The questionnaires were disseminated through professional healthcare networks, online platforms, and patient advocacy groups.
- Responses were collected anonymously to encourage candid feedback.
- Quantitative questions used Likert-scale ratings to facilitate trend analysis, while open-ended responses provided nuanced insights.

By adopting this dual-questionnaire approach, the ENTRUST project ensured that the diverse experiences and needs of both healthcare professionals and patients were captured, creating a robust foundation for developing frameworks that address trustworthiness, cybersecurity, and ethical standards in CMDs.

3.2.5.3 Questionnaires Results

The analysis of the questionnaire results provided valuable insights into the perceptions and opinions of end users (clinicians and expert users) and citizens (patients) regarding the trustworthiness and cybersecurity of CMDs. To facilitate better analysis, the responses from the two target groups were classified into thematic categories that reflect the core aspects of CMD usability, security, transparency, and ethical compliance.

3.2.5.3.1 End Users – Technology Users

A total of 51 responses were received from end users, including clinicians, biomedical engineers, and IT professionals, providing insights into the usability, security, and trustworthiness of CMDs.

- **Usability and Accessibility**
  - **Ease of Use**: 68% of respondents rated CMDs as “Easy” or “Very Easy” to use, with 22% marking them as “Neutral” and 10% indicating difficulties. This reflects positive overall usability but highlights areas where user interfaces could be simplified further.
  - **User Accessibility**: 72% of respondents agreed or strongly agreed that CMDs are designed with accessibility in mind. However, 15% disagreed, citing issues with accommodating diverse user needs.

Funded by the Horizon Framework Programme of the European Union

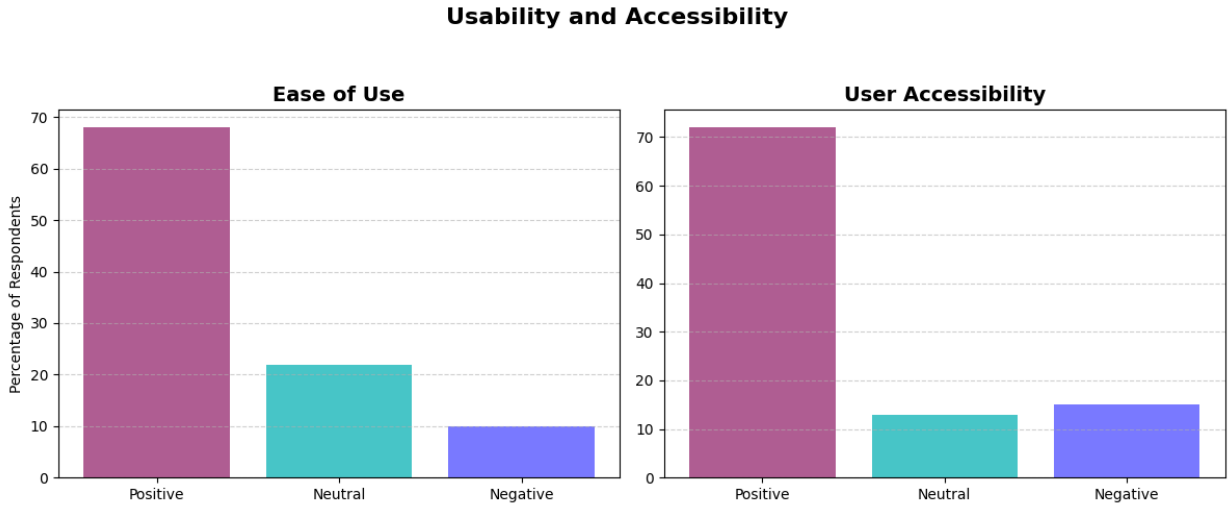

Figure 14: Usability and Accessibility Metrics - End Users/Technology Users

- **Data Security and Privacy**
  - **Confidence in Data Protection**: 58% of respondents reported being "Somewhat Confident" or "Very Confident" in the protection of personal and health data by CMDs, but 30% expressed slight or significant concerns.
  - **Informed Data Usage**: Only 45% felt "Fully Informed" or "Somewhat Informed" about how their data is used, indicating a need for improved communication on data management policies.

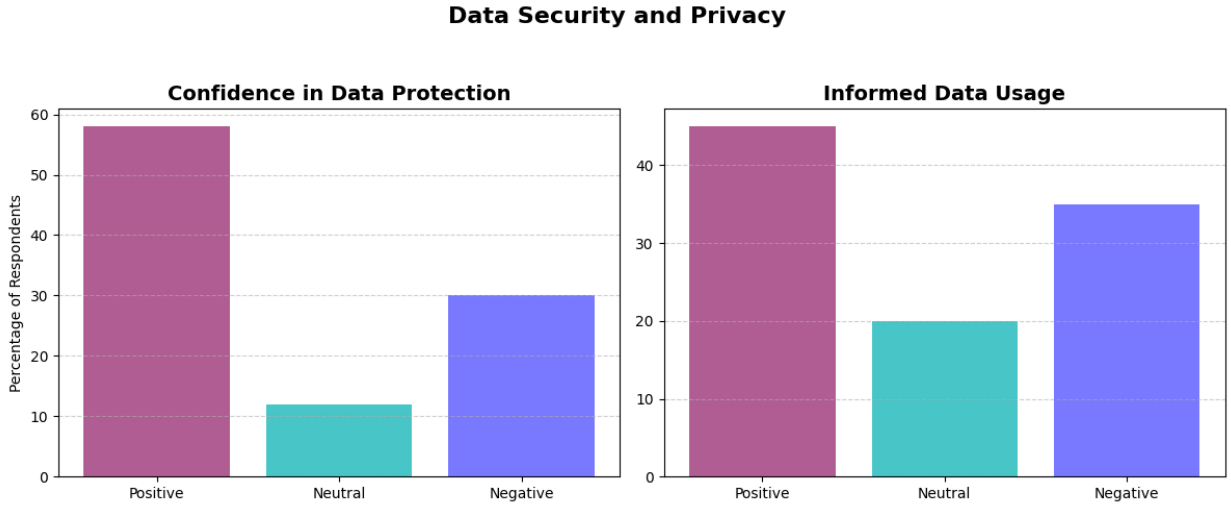

Figure 15: Data Security and Privacy Perceptions - End Users/Technology Users

- **Transparency and Trust**
  - **Trust in Critical Situations**: 64% of respondents expressed "Full" or "Mostly Trust" in CMD reliability during critical situations, while 20% indicated slight

Funded by the Horizon Framework Programme of the European Union

distrust, suggesting opportunities to build confidence through rigorous testing and transparent reporting.

- **Perception of Cybersecurity Standards**: 55% agreed or strongly agreed that CMDs adhere to high cybersecurity standards, while 25% were neutral, and 20% expressed concerns.

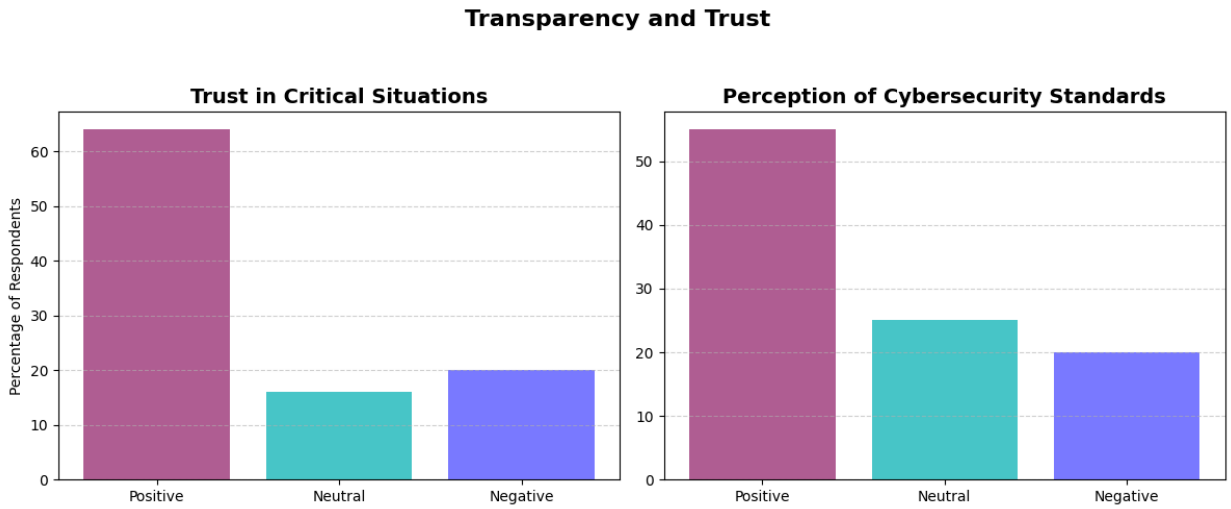

Figure 16: Transparency and Trust in CMDs - End Users/Technology Users

- **Suggestions for Improvement**

  Respondents frequently suggested:

  - Simplifying user interfaces to improve accessibility.
  - Providing clearer communication regarding data security measures.
  - Enhancing training resources to address potential user errors.
  - Developing features that improve integration across diverse healthcare settings.

3.2.5.3.2 Citizens – Patients

A total of **112 responses** were collected from patients and citizens, focusing on their perspectives regarding CMDs' transparency, security, and ethical compliance.

- **Awareness and Transparency**
  - **Understanding of CMDs**: 62% of respondents felt "Very Well Informed" or "Somewhat Informed" about the purpose and functioning of CMDs, while 25% were "Neutral" and 13% felt poorly informed, suggesting the need for improved educational materials.
  - **Transparency on Data Collection**: 58% agreed or strongly agreed that CMDs provide sufficient transparency about data collection, but 28% expressed doubts.

Funded by the Horizon Framework Programme of the European Union

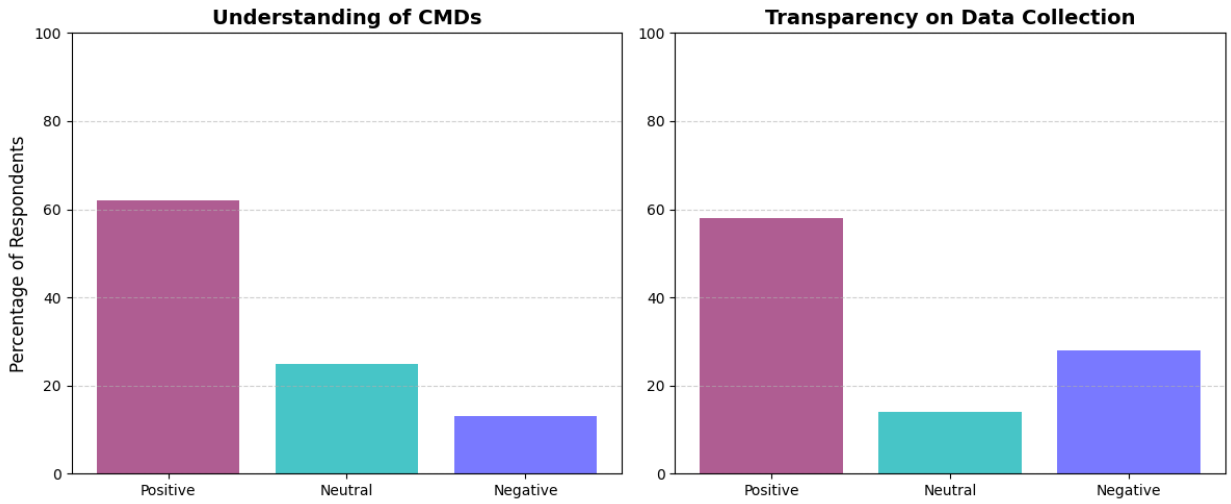

Figure 17: Understanding of CMDs and Transparency on Data Collection - Citizens/ Patients

- **Perceived Security and Privacy**
  - **Sense of Security**: 66% of respondents felt “Very Secure” or “Somewhat Secure” about the protection of their sensitive health data, while 22% indicated insecurity, pointing to room for improvement in addressing patient concerns.
  - **Satisfaction with Privacy Safeguards**: 60% were “Satisfied” or “Very Satisfied,” while 25% were neutral, and 15% expressed dissatisfaction, particularly regarding data sharing policies.

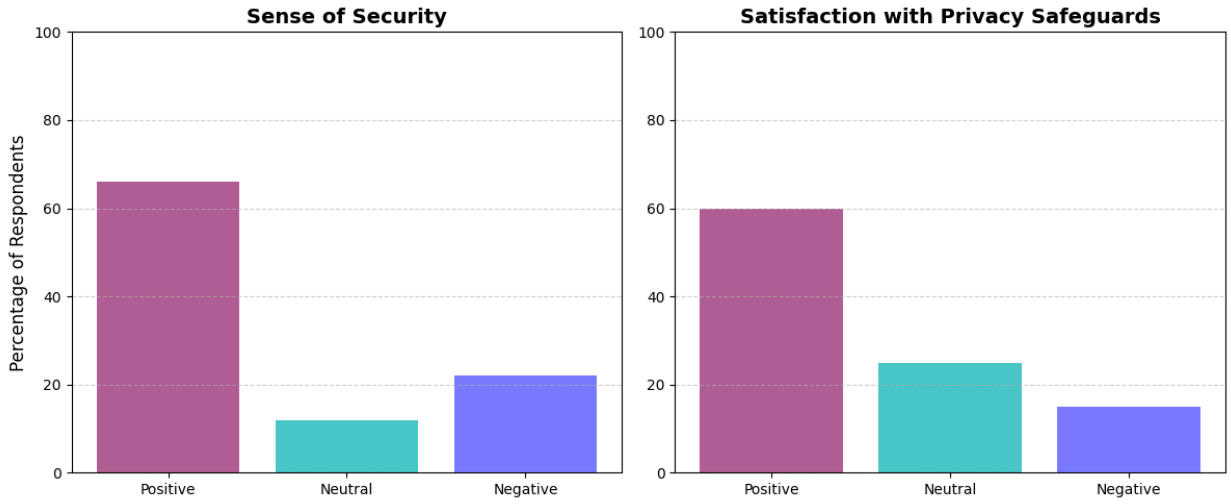

Figure 18: Sense of Security and Satisfaction with Privacy Safeguards - Citizens/ Patients

- **Ethical and Legal Compliance**
  - **Confidence in Compliance**: 63% of respondents believed CMDs comply with ethical and legal standards for data privacy, while 20% were neutral, and 17% expressed concerns.

Funded by the Horizon Framework Programme of the European Union

- **Trust in Ethical Practices**: 65% expressed “Full” or “Mostly Trust” in CMDs to operate ethically, with 20% indicating slight distrust.

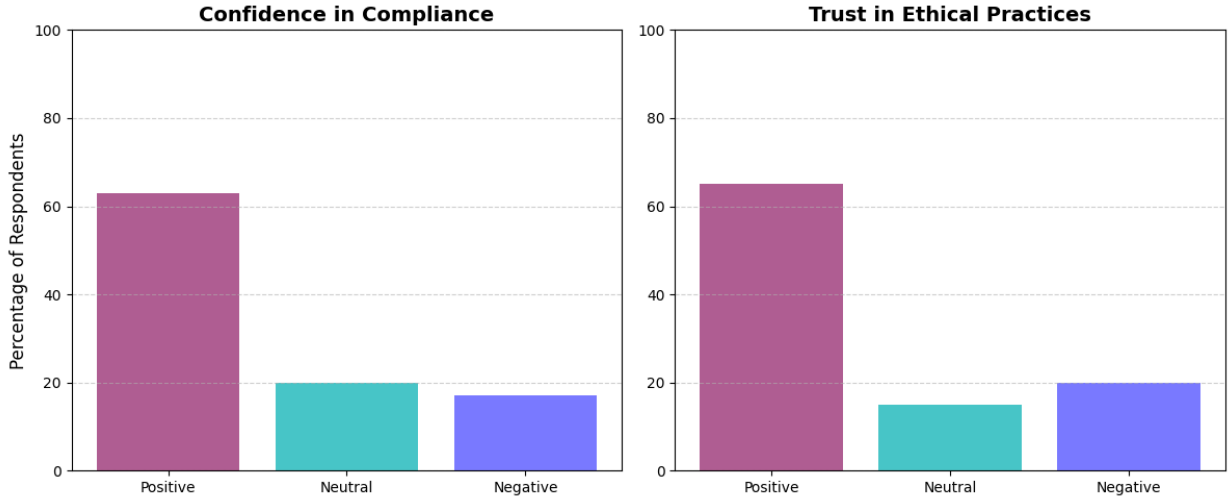

Figure 19: Confidence in Compliance and Trust in Ethical Practices - Citizens/ Patients

- **Suggestions for Improvement**

  Citizens suggested:

  - Enhancing transparency around data collection and usage.
  - Clearly communicating cybersecurity measures to build confidence.
  - Strengthening privacy safeguards, particularly concerning third-party data sharing.
  - Offering interactive educational resources to improve awareness of CMD functionality and data handling.

3.2.5.3.3 Combined Key Findings

- Both target groups highlighted the critical importance of **transparent communication** regarding CMD functionality, data management, and cybersecurity practices. Clear and consistent messaging was identified as a key driver of trust.
- **Cybersecurity vulnerabilities** were a shared concern across groups, with respondents calling for **enhanced usability, robust privacy protections**, and clear accountability mechanisms.
- Trust frameworks, such as in the **ENTRUST** case, were positively received by both end users and citizens as a **dynamic solution** to address these challenges, offering adaptability to evolving threats and fostering confidence in CMDs.
- **User-centric design** was emphasised by end users, particularly clinicians and healthcare professionals, who noted the need for CMDs to integrate seamlessly into clinical workflows without compromising security.

Funded by the Horizon Framework Programme of the European Union

- Citizens underlined the importance of **ethical and legal compliance** in data handling, with a focus on maintaining privacy and ensuring transparency about the purposes and uses of collected data.

The results reinforce the need to prioritise user-centric design, robust cybersecurity measures, and transparent communication in CMD development and deployment. These actionable insights align closely with the objectives of the ENTRUST project, ensuring the creation of trustworthy CMDs that effectively meet the needs of both end users and citizens. To build on these findings and capture a broader spectrum of perspectives, the questionnaires will continue to be distributed to a wider audience. This iterative approach will allow the ENTRUST project to adapt and refine its strategies, remaining responsive to the evolving needs and concerns of all stakeholders while reinforcing its commitment to ethical and secure CMD development.

3.3 Designing systems for society readiness

The design and implementation of cybersecurity measures in CMDs require a comprehensive approach that considers societal values, ethical considerations, and legal requirements. This involves not only technical proficiency but also a deep understanding of societal expectations and user perspectives. Addressing these complexities ensures the systems are not only functional but also socially desirable, ethically sound, and legally compliant.

3.3.1 Challenges in Designing for Society Readiness

The process of designing systems for societal readiness faces several challenges:

- **Uncertainty in User Perception**: Understanding how future users perceive security, privacy, and usability remains a significant challenge during the early stages of development.
- **Unforeseen Usage Practices**: Anticipating how users will apply a system and the unintended behaviours that may emerge is often difficult.
- **Translating Values into Design**: Effectively embedding cultural, ethical, and societal values into the functionality of systems is a complex task.
- **Avoiding Unintended Consequences**: Predicting and mitigating unintended societal impacts while still in the design phase is critical to ensuring system readiness.

3.3.2 Key Frameworks for Societal Readiness

Responsible Research and Innovation (RRI) provides a guiding framework for aligning research and innovation with societal needs and values. It emphasises anticipation, reflexivity, inclusion, and responsiveness as core principles:

- **Anticipation**: Examining both intended and unintended consequences of technological solutions, prompting "what if" questions to prepare for uncertainties.

Funded by the Horizon Framework Programme of the European Union

- **Reflexivity**: Challenging assumptions, examining underlying motivations, and being open to alternative solutions and approaches.
- **Inclusion**: Engaging end-users and stakeholders early and continuously in the design process to ensure their needs and perspectives shape the outcomes.
- **Responsiveness**: Incorporating insights gained through engagement and reflection to iteratively refine the design and implementation of systems.

3.3.3 Integrating System Engineering Thinking and Design Thinking

Systems engineering thinking is central to addressing these challenges. It advocates for a holistic approach that considers the interplay between technical, societal, and ethical dimensions throughout the lifecycle of CMDs. **Design thinking**, on the other hand, ensures a user-centric approach, fostering innovation while addressing real-world problems. **Co-creation** is another critical element in this process, actively involving stakeholders, including end-users such as clinicians and expert users, throughout the design and validation phases. This collaborative approach enhances usability and trust, ensuring that systems meet both functional and societal expectations.

3.3.4 Feedback Integration and Validation

Integrating end-user feedback during iterative design phases is essential to refine usability and security features. Cross-validation of design elements with stakeholders ensures alignment with societal values and practical requirements. Regular testing against **legal and ethical guidelines** and adherence to standards guarantee compliance and foster trust.

Designing systems for societal readiness requires a balanced approach that integrates technical innovation with societal, ethical, and legal considerations. By employing frameworks like RRI, adopting co-creation and systems engineering thinking, and rigorously validating through user feedback and standards compliance, the ENTRUST project ensures CMDs are not only effective but also aligned with the broader values and needs of society.

4 ENTRUST Contributions to Legal, Ethical, and Regulatory Frameworks

4.1 ENTRUST as a facilitator of regulatory compliance certification: liaison with data protection authorities and international bodies

As part of the legal and ethical compliance activities of ENTRUST, as well as within the scope of the project's efforts towards standardization and impact generation, Mandat International has participated in several international conferences (see table below) to present the ENTRUST project and its innovative certification-oriented approach to key stakeholders, particularly towards

Funded by the Horizon Framework Programme of the European Union

data protection authorities and international bodies surrounding the certification ecosystem (e.g. international accreditation authorities).

Table 1: ENTRUST as a facilitator of regulatory compliance certification - Conferences

Date	Conference Name	Location	Link	Estimated Participants	Description & Stakeholders
22-24 May 2024	CPDP (Computers, Privacy & Data Protection)	Brussels, Belgium	cpdpconferences.org	1,500+	A leading multidisciplinary conference on privacy and data protection, attracting academics, policymakers, industry leaders, and civil society representatives worldwide.
10-14 June 2024	Privacy Symposium Conference	Venice, Italy	privacysymposium.org	1,000+	Focuses on privacy, data protection, and compliance, drawing regulators, tech professionals, and legal experts globally.
1-10 October 2024	IAF-ILAC Joint Annual Meetings	Berlin, Germany	ilaciafmeetings.org	1,200+	An international conference on accreditation and conformity assessment, attracting experts, assessors, and industry professionals.
28 Oct-1 Nov 2024	Global Privacy Assembly (GPA)	Jersey, UK	gpajersey.com	1,500+	A major annual gathering of global data protection authorities and policymakers to address privacy challenges and frameworks.
20-21 November 2024	IAPP Europe Data Protection Congress	Brussels, Belgium	iapp.org	2,000+	A key European event for privacy professionals, covering GDPR developments and data protection trends, including industry leaders.

Funded by the Horizon Framework Programme of the European Union

Participation in these forums involved specialized presentations, bilateral discussions, and demonstrations of the proof-of-concept integration of the ENTRUST model with Europrivacy, the European Data Protection Seal. These initiatives were exceptionally effective, generating considerable interest from key stakeholders concerning the project enablers. Certification agencies and accrediting authorities shown significant interest in the prospective application of ENTRUST findings to enhance conventional certification procedures.

Participation in these events resulted in invites to return and enhance future iterations of these forums. This continuous involvement provides chances to demonstrate ENTRUST's outcomes as the project progresses into its exploitation phase, hence increasing exposure and possibility for acceptance within the wider certification and data protection community.

Moreover, ENTRUST's participation in these activities—especially at the Global Privacy Assembly (GPA) in Jersey—was essential in enabling the approval of the GPA resolution. This resolution urges international data protection authorities to contemplate certification schemes as a method to exhibit adherence to relevant statutory frameworks. This result highlights the strategic significance and influence of ENTRUST's efforts to enhancing certification procedures in data security and privacy.

4.2 Legal and Ethical Alignment in ENTRUST

The ENTRUST consortium is fully committed to aligning its activities with both legal and ethical frameworks to ensure the trustworthy development and deployment of CMDs. By adhering to European, international and national legislation, the consortium ensures compatibility with the directives and regulations relevant to the countries where data collection and system implementation take place. Key considerations include compliance with the EU e-Privacy Directive (2002/58/EC), GDPR (Regulation 2016/679), Directive 2016/680, and the Charter of Fundamental Rights of the European Union. In addition, ENTRUST follows Horizon 2020 ethical guidelines, including the Rules for Participation, ethics self-assessment guidance, and ethical principles outlined in the Model Grant Agreement. The consortium remains vigilant about ethical issues, such as consent for data collection, privacy preservation, and the secure storage and transfer of personal data. These measures ensure the safeguarding of individuals' identities and the ethical handling of sensitive information. Detailed legal and ethical requirements for ENTRUST activities are thoroughly addressed in deliverables D2.1 “ENTRUST Reference Architecture – Initial Release” and D2.2 “ENTRUST Reference Architecture – Final Release,” which outline compliance mechanisms and adherence to all applicable regulations. The ENTRUST consortium emphasises ethical issues surrounding evidence measures and trustworthiness in CMDs. By ensuring alignment with current medical standards, the project incorporates enhanced Conformance Certificates to validate compliance. These certificates

Funded by the Horizon Framework Programme of the European Union

integrate assurance claims to address ethical and legal requirements effectively, fostering trust in CMDs. Moreover, ENTRUST places responsibility on relevant partners to document and ensure compliance with local regulations, ethical guidelines, and data protection requirements, as mandated by their respective ethical boards and data protection authorities. This approach ensures the project not only meets current legal standards but also embodies the principles of responsible research and innovation, promoting trust among all stakeholders involved.

4.3 ENTRUST Recommendations

4.3.1 Proposal by ENTRUST for Revision of the Current Guidance (MDCG 2019–16)

In response to the increasing technological challenges linked to cybersecurity risks in medical devices, the ENTRUST consortium has identified areas for improvement in the current MDCG guidance document MDCG 2019–16. This guidance document, developed to align with the Medical Device Regulations (MDR 745/2017) and In Vitro Diagnostic Medical Device Regulations (IVDR 746/2017), outlines essential safety and security requirements for medical devices. However, ENTRUST has identified gaps in the standardisation of IT security and trustworthiness in medical devices and proposes amendments to the guidance through a White Paper.

Key observations of the ENTRUST proposal include:

1. **Defining Essential Requirements for Device Design**: There is a need to explicitly specify software and firmware requirements, secure communication protocols, and secure-by-design environments to enhance device safety and security.
2. **Formal Verification of Device Design**: Establishing a minimum set of requirements and supporting Trusted Components (TCs) can assist in the formal verification of medical device designs, ensuring robust cybersecurity and operational integrity.
3. **Risk-Benefit Analysis**: Manufacturers must incorporate a risk-benefit framework that balances safety, performance, and security in the design and deployment of CMDs.
4. **Establishing Trustworthiness**: A comprehensive model of trustworthiness that integrates safety, security, privacy, resilience, and reliability is essential. ENTRUST highlights the challenge of defining trust requirements without compromising device functionality.

The ENTRUST recommendations for revising MDCG 2019–16 include:

- Expanding the notion of **Conformity Certificates** to include runtime and verifiable evidence of device security and trustworthiness.
- Harmonising the **Conformity Assessment Framework** to include runtime claims provided by medical devices.
- Enhancing Manufacturer Usage Descriptions (MUDs) with **Protection Profiles**, serving as verifiable evidence of device security posture.

Funded by the Horizon Framework Programme of the European Union

- Establishing a set of **minimum-security requirements** for device capabilities, such as trusted/secure boot mechanisms.

These proposed changes aim to harmonise cybersecurity management in medical devices, enabling manufacturers and healthcare organisations to maintain secure, interconnected, and large-scale device operations.

This proposal is also detailed in D1.2, where readers can find additional insights and explanations about ENTRUST's recommendations and their alignment with legal and ethical frameworks.

4.3.2 Recommendations from Project Activities and Open Access Initiatives

The ENTRUST project has consistently emphasised the importance of inclusivity and accessibility in its methodologies and outputs. Based on project activities, workshops, questionnaires, and interactions with stakeholders, the following recommendations aim to engage a broader range of end-users and stakeholders, particularly those who may hesitate to participate due to the complexity or perceived barriers associated with medical device cybersecurity and trust management.

- **Enhancing Awareness and Accessibility**:
  - Simplify technical language and present project deliverables in user-friendly formats to make the content accessible to non-technical stakeholders, such as patients and smaller healthcare providers.
  - Develop educational resources, including webinars, visual guides, and explainer videos, to demystify concepts like cybersecurity standards, trust frameworks, and conformity assessments.
  - Leverage open-source platforms and tools to provide stakeholders with hands-on experience in secure CMD implementation and evaluation.
- **Strengthening Stakeholder Engagement**:
  - Establish ongoing dialogue channels, such as forums, surveys, and focus groups, to continuously gather feedback from diverse end-users, including patients, clinicians, and technology providers.
  - Collaborate with professional associations, patient advocacy groups, and medical organisations to expand the reach of project activities and ensure the inclusion of underrepresented stakeholders.
- **Promoting Co-Creation and Inclusivity**:
  - Involve end-users directly in the design, testing, and validation of CMD solutions to ensure their needs and concerns are adequately addressed.
  - Foster a co-creation approach where stakeholders, including patients and experts, actively contribute to the development of user-centric trust frameworks and cybersecurity solutions.

Funded by the Horizon Framework Programme of the European Union

- Facilitate multidisciplinary workshops and training sessions to bridge the gap between technical developers and non-technical users.

- **Leveraging Open Access and Open-Source Solutions**:
  - Expand the adoption of open-source components, allowing stakeholders to examine, adapt, and implement cybersecurity measures with transparency.
  - Provide step-by-step implementation guides to help healthcare providers and manufacturers integrate ENTRUST's solutions without requiring extensive prior expertise.
  - In alignment with the European Commission's support for open access, ensure that all scientific information, including data, reports, and software generated by ENTRUST, is freely accessible and reusable. This practice enhances transparency, fosters innovation, and maximises the societal impact of project outputs.
- **Building Trust through Transparency**:
  - Clearly communicate the benefits and limitations of CMD cybersecurity measures, helping end-users understand what protections are in place and what risks remain.
  - Regularly publish project progress and updates in accessible formats, ensuring transparency in methodologies and outcomes.
- **Encouraging Broader Adoption through Demonstrations**:
  - Organise live demonstrations of ENTRUST's trust assessment frameworks and cybersecurity solutions to showcase their practical applications and ease of use.
  - Develop case studies that illustrate successful implementation of ENTRUST components in real-world healthcare scenarios, highlighting measurable benefits in trust, security, and usability.

By integrating the European Union's commitment to open access and fostering an inclusive, transparent, and co-creative environment, ENTRUST aims to bridge the gap between complex technical solutions and the practical needs of stakeholders. These efforts ensure that the project outputs remain accessible, engaging, and impactful, enabling all stakeholders to confidently participate in shaping the future of secure and trustworthy CMDs.

4.4 Gender Equality

ENTRUST is committed to promoting gender equality in line with Article 33 of the Grant Agreement and the EU's Policy on Equal Opportunities, as outlined in Articles 2 and 3 of the Treaty on the European Union and the Gender Equality Strategy 2020–2025. The project ensures balanced representation across leadership roles, with women holding key positions in project coordination, ethics, technical, and innovation management. Gender balance is a key priority within the ENTRUST project, and we are committed to fostering an inclusive and equitable

Funded by the Horizon Framework Programme of the European Union

environment. We aim for balanced representation across Work Package and Task Leadership roles. Current efforts reflect significant progress toward achieving gender equality, ensuring meaningful participation from both male and female contributors at all levels. ENTRUST guarantees equal involvement of all genders in defining requirements, designing, and developing CMDs, ensuring outcomes address diverse end-users equitably. Additionally, the project fosters work-life balance and implements gender-sensitive practices throughout its activities, contributing to a more inclusive and equitable healthcare and technology landscape.

5 Conclusions

The deliverable has outlined the ENTRUST project's robust approach to addressing legal, ethical, and societal dimensions in the development and deployment of CMDs. Through an exploration of relevant EU and international regulations, the project demonstrates its commitment to compliance, ensuring the security, privacy, and trustworthiness of its solutions. The ENTRUST framework integrates legal and ethical requirements from directives such as the GDPR, the e-Privacy Directive, and the Cybersecurity Act, alongside industry-specific regulations like the MDR. The analysis of these frameworks and their incorporation into the project underscores ENTRUST's dedication to safeguarding sensitive health data and fostering trust among stakeholders. Ethical considerations, such as informed consent, privacy preservation, and transparency, have been systematically embedded into all aspects of the project. The project's dynamic Conformance Certificates ensure the alignment of CMDs with current medical standards, providing a comprehensive mechanism for evidence-based trust and compliance. The deliverable also highlights the significance of engaging end-users and citizens in the design and validation process. Insights gathered from workshops and questionnaires revealed critical areas for improvement, particularly in usability, transparency, and cybersecurity, while confirming strong public support for trust frameworks like ENTRUST. These findings have been instrumental in shaping the project's iterative development process. Furthermore, ENTRUST's recommendations for revising current guidance, such as MDCG 2019-16, advocate for harmonised cybersecurity standards and methodologies. These proposals reflect the consortium's proactive stance in addressing gaps and advancing the state of the art in CMD development. Finally, ENTRUST's commitment to gender equality reinforces its holistic approach to inclusivity and innovation. By ensuring balanced representation and addressing gender-specific needs, the project sets a benchmark for equitable healthcare and technological advancements. ENTRUST exemplifies a forward-looking, interdisciplinary approach to addressing the complex legal, ethical, and societal challenges in CMD development. By fostering trust, ensuring compliance, and promoting inclusivity, ENTRUST paves the way for a more secure and equitable future in healthcare technology. The insights and frameworks presented in this deliverable will serve as a foundation

Funded by the Horizon Framework Programme of the European Union

for ongoing research, stakeholder engagement, and policy alignment, ensuring that ENTRUST's impact extends beyond the project's lifetime.

References

[1] ENTRUST, "D1.4 ENTRUST's Data Management Plan," 2024.
[2] ENTRUST, "D2.1 ENTRUST Reference Architecture – Initial Release," 2024.
[3] ENTRUST, "D2.2 ENTRUST Reference Architecture – Final Release," 2024.
[4] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." OJ L 119, Dec. 04, 2016.
[5] E. Union, "Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance)," 2023. [Online]. Available: http://data.europa.eu/eli/reg/2023/2854/oj
[6] E. Union, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space," 2017. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197
[7] G. Gonz'alez Fuster, "Privacy and the Protection of Personal Data Avant la Lettre," in *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol. 16, Springer, Cham, 2014. doi: 10.1007/978-3-319-05023-2_2.
[8] E. Union, "Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.)," 2017. [Online]. Available: http://data.europa.eu/eli/reg/2017/745/oj
[9] E. Union, "Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.)," 2017. [Online]. Available: http://data.europa.eu/eli/reg/2017/746/oj
[10] E. Union, "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)," 2022. [Online]. Available: http://data.europa.eu/eli/reg/2024/1689/oj
[11] E. Union, "Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance)," 2022. [Online]. Available: http://data.europa.eu/eli/reg/2022/868/oj
[12] E. Union, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)," 2019. [Online]. Available: http://data.europa.eu/eli/reg/2019/881/oj
[13] "Consolidated text: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)Text with EEA relevance," 2022. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/2022-12-27
[14] E. Union, "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)." [Online]. Available: http://data.europa.eu/eli/reg/2024/2847/oj
[15] E. Union, "Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council

Funded by the Horizon Framework Programme of the European Union

as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC),” 2024. [Online]. Available: http://data.europa.eu/eli/reg_impl/2024/482/oj
[16] CISCO, “NIS2 Compliance for Industries White Paper.” 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/industrial-security/network-info-security-wp.html
[17] M. D. C. Group, “MDCG 2019-16 Guidance on Cybersecurity for medical devices,” 2019.
[18] E. Union, “Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance,” 2014. [Online]. Available: http://data.europa.eu/eli/dir/2014/53/oj
[19] E. Commission, “Ethics guidelines for trustworthy AI,” 2019. doi: 10.2759/346720.
[20] HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, “THE ASSESSMENT LIST FOR TRUSTWORTHY ARTIFICIAL INTELLIGENCE (ALTAI),” 2019. doi: 10.2759/002360.
[21] Council of Europe, “Convention 108 + Convention for the protection of individuals with regard to the processing of personal data,” 2018. [Online]. Available: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
[22] R. Cagan, “The San Francisco Declaration on Research Assessment,” *Dis Model Mech*, vol. 6, no. 4, pp. 869–870, Jul. 2013, doi: 10.1242/dmm.012955.
[23] E. Union, “Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),” 2022. [Online]. Available: http://data.europa.eu/eli/dir/2002/58/oj
[24] N. Smuha *et al.*, “How the EU can achieve legally trustworthy AI,” *SSRN*, 2021.
[25] K. L. G. Snider, R. Shandler, S. Zandani, and D. Canetti, “Cyberattacks, cyber threats, and attitudes toward cybersecurity policies,” *Journal of Cybersecurity*, vol. 7, no. 1, p. tyab019, Oct. 2021, doi: 10.1093/cybsec/tyab019.
[26] E. Politou, E. Alepis, M. Virvou, and C. Patsakis, “Privacy and Personal Data Protection,” in *Privacy and Data Protection Challenges in the Distributed Era*, vol. 26, Springer, Cham, 2022. doi: 10.1007/978-3-030-85443-0_2.
[27] N. Kostyuk and C. Wayne, “The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public,” *Journal of Global Security Studies*, vol. 6, no. 2, p. ogz077, Mar. 2021, doi: 10.1093/jogss/ogz077.
[28] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, “Cybersecurity and healthcare: how safe are we?,” *BMJ*, p. j3179, Jul. 2017, doi: 10.1136/bmj.j3179.
[29] A. T. Alanazi, “Clinicians’ Perspectives on Healthcare Cybersecurity and Cyber Threats,” *Cureus*, Oct. 2023, doi: 10.7759/cureus.47026.
[30] K. R. Ludvigsen, “The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions,” *Law Tech Hum*, vol. 5, no. 2, pp. 59–77, Nov. 2023, doi: 10.5204/lthj.3080.

Funded by the Horizon Framework Programme of the European Union