UNIVERSITY
INSTITUTE
OF LISBON

Establishing a EU Blockchain for Healthcare Data Requirements, Challenges, and Pathways to Cross-Border Interoperability

Alexandre Miguel Nobre Ramos Leitão

Master in Digital Technologies for Business

Orientador:
Professor Doutor João Carlos Amaro Ferreira,
Professor Auxiliar com Agregação,
ISCTE-IUL

December, 2025

Department of Information Science and Technology

Establishing a EU Blockchain for Healthcare Data Requirements, Challenges, and Pathways to Cross-Border Interoperability

Alexandre Miguel Nobre Ramos Leitão

Master in Digital Technologies for Business

Supervisor:
Professor Doutor João Carlos Amaro Ferreira,
Professor Auxiliar com Agregação,
ISCTE-IUL

December, 2025

Acknowledgements

I would like to thank my colleagues Rui and Alexandre for their companionship, encouragement, and presence during the time spent working on this dissertation.

Abstract

Demand for trustworthy, cross-border access to electronic health data in the European Union is increasing, driven by stringent privacy obligations under the General Data Protection Regulation and the European Health Data Space policy agenda. Fragmented national infrastructures and heterogeneous practices still hinder lawful, timely sharing between Member States. This dissertation proposes a central European Union coordination layer, conceived as a permissioned blockchain that records only minimal, non-identifying metadata, to deliver deterministic authorisation and immutable audit for cross-border exchanges while keeping personal health data strictly off-chain.

Guided by the Design Science Research Methodology, the work develops requirements, a four-layer reference architecture, and a theory-based evaluation. The architecture comprises four layers: Platform and Consensus, which uses a permissioned Practical Byzantine Fault Tolerance mechanism to ensure finality, deterministic ordering, and qualified timestamps; Identity and Membership, based on organisational credentials recognised under the electronic Identification, Authentication and Trust Services Regulation; Minimal Data Model and Authorisation Services, which cover consent presence and lifecycle, deterministic allow/deny decisions, narrowly scoped emergency access, and first-class revocation; and Audit, Evidence and Governance, which provide tamper-evident episode narratives and transparent change control. National relays and, where needed, a European Union access gateway interface at the perimeter with identical central semantics.

Evaluation is conducted theoretically through continuous use-case narratives, including registering an access intent, issuing an authorisation decision, auditing an episode end-to-end, break-glass access, and revocation. These are assessed against three lenses: regulatory compliance, audit/evidence/oversight, and privacy by design and proportionality.

Keywords: EU health data; GDPR; EHDS; eIDAS; Permissioned blockchain; Authorisation; Audit; Cross-border interoperability.

Resumo

A procura de acesso fiável e transfronteiriço a dados de saúde eletrónicos na União Europeia está a aumentar, impulsionada por obrigações rigorosas de privacidade ao abrigo do Regulamento Geral sobre a Proteção de Dados e pela agenda política do Espaço Europeu de Dados de Saúde. A fragmentação das infraestruturas nacionais e a heterogeneidade de práticas continuam a dificultar a partilha lícita e atempada entre Estados-Membros. Esta dissertação propõe uma camada central de coordenação à escala da União Europeia, concebida como uma *permissioned blockchain* que regista apenas metadados mínimos e não identificativos, para assegurar uma autorização determinística e uma auditoria imutável nas trocas transfronteiriças, mantendo os dados pessoais de saúde estritamente fora da cadeia.

Orientado pela Metodologia de Investigação em Ciência do Design, o trabalho desenvolve requisitos, uma arquitetura de referência de quatro camadas e uma avaliação baseada em teoria. A arquitetura integra quatro camadas: Plataforma e Consenso, que utiliza um mecanismo *Practical Byzantine Fault Tolerance* em regime *permissioned* para garantir finalidade, ordenação determinística e carimbos temporais qualificados; Identidade e Adesão, baseada em credenciais organizacionais reconhecidas ao abrigo do Regulamento relativo à Identificação Eletrónica, Autenticação e Serviços de Confiança; Modelo de Dados Mínimo e Serviços de Autorização, que abrangem a presença e o ciclo de vida do consentimento, decisões determinísticas de permitir/recusar, acesso de emergência de âmbito estritamente delimitado e revogação como capacidade de primeira ordem; e Auditoria, Evidência e Governação, que asseguram narrativas de episódios resistentes a adulteração e um controlo de alterações transparente. Os relés nacionais e, quando necessário, um *gateway* de acesso da União Europeia na periferia interligam-se com semântica central idêntica.

A avaliação é conduzida de forma teórica através de narrativas contínuas de casos de uso, incluindo o registo de uma intenção de acesso, a emissão de uma decisão de autorização, a auditoria de um episódio de ponta a ponta, o acesso de emergência (*break-glass*) e a revogação. Estas narrativas são analisadas segundo três perspetivas: conformidade regulamentar, auditoria/evidência/supervisão e privacidade desde a conceção e proporcionalidade.

Palavras-chave: Dados de saúde na UE; RGPD; EHDS; eIDAS; Blockchain permissionada; Autorização; Auditoria; Interoperabilidade transfronteiriça.

Index

Acknowledgements i
Resumo iii
Abstract v
Index vii
Figure Index ix
Table Index xi
Acronmys xiii

CHAPTER 1. Introduction 1
1.1. Motivation 1
1.2. Problem Identification 2
1.3. Objectives 3
1.4. Research Questions 4
1.5. Key Concepts 4

CHAPTER 2. Literature Review 7
2.1. PRISMA Methodology 7
2.2. Literature Review 8
2.2.1. Blockchain 11
2.2.2. Healthcare 13
2.3. Blockchain in EU Healthcare: Real-World Use Cases 15
2.3.1. Estonia: Nationwide Blockchain-Secured Health Records 15
2.3.2. Pan-European PharmaLedger: Trusted Medicine Supply Chains 16
2.4. Critical Reflection and Positioning of This Research 17

CHAPTER 3. Requirements & Architecture 19
3.1. DSRM Methodology 19
3.2. Central Coordination Layer 19
3.3. Participants 20
3.3.1. EU Members 20
3.3.2. EU (Consortium & Trust Services) 21
3.3.3. Patients 21

3.3.4. Auditor(s) 21
3.4. Functional Requirements 22
3.5. Non-Functional Requirements 23
3.6. EU Central Blockchain Architecture 25
3.7. Smart Contracts 27
CHAPTER 4. Evaluation 29
4.1. Evaluation Approach 29
4.1.1. Regulatory Compliance 29
4.1.2. Audit, Evidence, and Oversight 30
4.1.3. Privacy by Design and Proportionality 30
4.2. Use Cases 30
4.2.1. Use Case 1: Register the Request 31
4.2.2. Use Case 2: Accepting the request 32
4.2.3. Use Case 3: Auditing the request 33
4.2.4. Use Case 4: Break-glass request 34
4.2.5. Use Case 5: Revoking the request 35
4.3. Real World Use Case Example 37
4.3. GDPR Alignment 39
CHAPTER 5. Conclusions 41
5.1. Restatement of the Problem and Objectives 41
5.2. Positioning of My Thesis and Its Contribution 42
5.3. Answers to the Research Questions 42
5.4. Practical Implications for Member States 45
5.5. Limitations and Threats to Validity 46
5.6. Risk Considerations and Mitigations 46
5.7. Future Work 48
5.8. Final Remarks 49

Bibliographic References 51

Figure Index

Figure 1 - PRISMA instance of the literature review 8
Figure 2 - Number of documents before screening 9
Figure 3 - Design Science Research Methodology (Peffers et al.) 19
Figure 4 - Central Chain 26
Figure 5 - Use case 1 Diagram example of communication 32
Figure 6 - Use case 2 Diagram example of communication 33
Figure 7 - Use case 3 Diagram example of communication 34
Figure 8 - Use case 4 Diagram example of communication 35
Figure 9 - Use case 5 Diagram example of communication 36

Table Index

Table 1 - Summary of documents 9
Table 2 - Functional Requirements 22
Table 3 - Non-Functional Requirements 23
Table 4 - NFR Justification 24
Table 5 - Smart Contracts 28
Table 6 - Functional Requirements Mapping 38
Table 7 - Smart Contracts used in Use Case 38

Acronyms

API	**A**pplication **P**rogramming **I**nterface
DSRM	**D**esign **S**cience **R**esearch **M**ethodology
EHDS	**E**uropean **H**ealth **D**ata **S**pace
EHR	**E**lectronic **H**ealth **R**ecords
EHRxF	**E**lectronic **H**ealth **R**ecord **E**xchange **F**ormat
eIDAS	**e**lectronic **I**dentification, **A**uthentication and Trust **S**ervices
ePI	**e**lectronic **P**roduct **I**nformation
EU	**E**uropean **U**nion
EUDI	**E**uropean **U**nion **D**igital **I**dentity
FHIR	**F**ast **H**ealthcare **I**nteroperability **R**esources
GDPR	**G**eneral **D**ata **P**rotection **R**egulation
HDAB	**H**ealth **D**ata **A**ccess **B**odies
HIPAA	**H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct
IoT	**I**nternet **o**f **T**hings
IT	**I**nformation **T**echnology
PBAC	**P**olicy-**B**ased **A**ccess **C**ontrol
PBFT	**P**ractical **B**yzantine **F**ault **T**olerance
PHI	**P**rotected **H**ealth **I**nformation
PoC	**P**roof **o**f **C**oncept
PoS	**P**roof **o**f **S**take
PoW	**P**roof **o**f **W**ork
PRISMA	**P**referred **R**eporting **I**tems for **S**ystematic **R**eviews and **M**eta-Analyses
SOA	**S**ervice-**o**riented **A**rchitecture

CHAPTER 1

Introduction

Healthcare data is increasingly generated and shared across various platforms and national borders, raising critical concerns about security, privacy, and interoperability. Conventional health information systems struggle with data fragmentation and siloed records, resulting in suboptimal interoperability and potential gaps in patient care continuity [1]. At the same time, the exponential growth of electronic health records has amplified the need for a safe, transparent, and efficient data management framework [1], [2]. Ensuring that sensitive patient information remains confidential and intact is paramount, especially as cyber-attacks and data breaches continue to pose grave threats to healthcare systems [1]. These challenges are accentuated in the European Union (EU), where cross-border health data exchange is envisioned but must adhere to strict data protection rules.

1.1. Motivation

The COVID-19 pandemic starkly exposed weaknesses in current healthcare Information Technology (IT) infrastructures and highlighted the urgent need for secure, interoperable, and flexible healthcare systems [2]. Even under normal conditions, patient mobility across EU member states calls for seamless health data exchange. However, today's healthcare providers often operate isolated data silos, which hinders information flow and coordination [3]. This fragmentation not only impedes care efficiency but also undermines the goal of a unified European Health Data Space [4] (EHDS). There is a clear impetus to modernise data-sharing mechanisms so that medical records can follow the patient across institutions and borders in a trustworthy manner.

Stakeholders have expressed dissatisfaction with existing data governance frameworks, such as ISO [5] standards, the General Data Protection Regulation (GDPR) [6] implementation, and the Health Insurance Portability and Accountability Act (HIPAA) [7], for effectively safeguarding healthcare data [1]. While the GDPR provides a strong legal foundation in Europe, enforcing its provisions (like obtaining explicit consent and enabling patient control over data use) remains challenging in practice. Organisations might fail to fully honour patients' consent preferences or even attempt to cover up data breaches under the current systems. These risks motivate the search for a technological solution that can guarantee accountability and transparency in data handling. By design, a blockchain-based ledger creates an immutable audit trail of all data access and exchange events. This could empower supervisory authorities in each

EU member state to verify compliance in real time and proactively detect any misuse or unauthorised access to personal health data [8].

1.2. Problem Identification

Implementing cross-border interoperability via blockchain requires addressing several interrelated problems in the current healthcare data ecosystem.

Data fragmentation and interoperability issues: Health records are dispersed across incompatible systems, making it challenging to aggregate a patient's records. Traditional architectures lead to isolated data silos, impeding the seamless exchange of medical information between providers and across countries [1], [3]. This lack of interoperability can delay treatment and reduce the quality of care when patients move between different healthcare systems.

Security and privacy vulnerabilities: Electronic health records and other sensitive data are prime targets for cyberattacks. Conventional IT systems often struggle to ensure the full spectrum of security requirements mandated by regulations. Key properties like confidentiality, integrity, fine-grained access control, and data anonymity are not uniformly guaranteed, especially once data leaves a provider's direct control [9]. Recent data breaches and unauthorised access incidents underscore the inadequacy of current measures [1], underscoring the need for new approaches to safeguard patient data against evolving threats.

Insufficient consent enforcement and auditability: Patients have the right to determine who accesses their health information, yet enforcing consent preferences throughout the data lifecycle is problematic in today's systems. Few solutions ensure that a patient's explicit consent directives are strictly followed and logged in a tamper-proof manner [8]. Likewise, auditing data use is labour-intensive and error-prone; it is often difficult for patients or regulators to trace how personal data has been used or shared. The lack of an immutable, verifiable chain of events for data handling leads to gaps in accountability [8], [2].

Cross-organisation trust and regulatory compliance: In a cross-border context, multiple actors (e.g. hospitals, labs, insurers, national authorities) need to collaborate while adhering to GDPR and other relevant regulations. Trust between these parties is not automatic, as each maintains its own records and audit logs. Ensuring that all parties comply with data protection rules and respect patient rights is difficult without a unified oversight mechanism. Current governance models rely on after-the-fact reporting and goodwill, which may fail to prevent non-compliance or deliberate data misuse. This problem is evident in the GDPR's breach notification model, which requires controllers to self-report incidents [8]. Without a better

system, a hospital might conceal violations, and authorities would have limited means to detect such behaviour in a timely fashion. As a result, a fundamental challenge is enabling trusted collaboration among organisations, patients, and regulators to handle health data [8].

1.3. Objectives

This thesis pursues three interrelated objectives that aim to address the limitations of cross-border healthcare data sharing within the European Union and evaluate the potential of blockchain technology in improving the management and exchange of healthcare data.

First, the thesis seeks to critically assess whether blockchain technology can meet the requirements of healthcare data management in a European context, especially under the regulatory frameworks governing data protection. This involves evaluating blockchain's strengths, such as decentralisation, immutability, and distributed trust, and considering how these can support secure and transparent data sharing while enforcing privacy. At the same time, it addresses blockchain's limitations, including concerns regarding scalability and complexity.

Second, the research conducts a comprehensive review of the existing literature and developments related to the use of blockchain in healthcare. This includes a survey of academic research, industry pilots, and case studies exploring blockchain applications in areas such as electronic health records (EHR), consent management, and the pharmaceutical supply chain. The review also incorporates the regulatory frameworks that govern health data in Europe, with a focus on GDPR, electronic Identification, Authentication and Trust Services (eIDAS), and EHDS, and how these regulations influence blockchain adoption. By synthesising current knowledge, the thesis identifies both best practices and existing gaps in the application of blockchain to healthcare data management in the EU context.

Lastly, the thesis aims to design and theoretically evaluate a conceptual solution architecture for a blockchain-based EU-level coordination layer for healthcare data exchange. The proposed architecture does not include a full-scale prototype. Instead, it uses design science research methodology to propose an architectural model that provides deterministic authorisation, immutable audit, and verifiable consent management for cross-border health data exchanges. This layer is intended to meet regulatory requirements while upholding privacy-by-design principles, with minimal on-chain data. The solution's potential to enable secure, transparent, and compliant cross-border data exchanges will be evaluated through theoretical use cases based on realistic healthcare scenarios.

In summary, this research has three main objectives:

- Validate blockchain as a viable solution for healthcare data management and compare it with alternative technologies.
- Review and systematise the body of knowledge on blockchain applications and relevant European regulations.
- To design and theoretically evaluate a conceptual blockchain-based coordination layer that tracks healthcare data securely and transparently across borders, aligned with regulatory compliance and privacy requirements.

1.4. Research Questions

This thesis investigates the potential of blockchain technology to address challenges in cross-border healthcare data exchange within the European Union. Specifically, it explores how blockchain can improve privacy, security, and interoperability while ensuring compliance with EU regulations. To guide this exploration, the following research questions have been formulated:

- How can blockchain technology address the current challenges in cross-border healthcare data exchange within the European Union?
- To what extent can a permissioned blockchain model enhance privacy and consent management of electronic health records in compliance with GDPR and other EU regulations?
- What are the functional and non-functional requirements for building a blockchain-based EU coordination layer for healthcare data exchange?

Together, these research questions will guide the investigation into how blockchain can address the complex issues surrounding cross-border healthcare data exchange in the European Union.

1.5. Key Concepts

Blockchain and Distributed Ledger Technology: Blockchain is a type of distributed ledger technology where data is organised in a chain of blocks that are cryptographically linked and replicated across a network of nodes. In a blockchain network, transactions (e.g., a doctor accessing a patient record) are grouped into blocks, and each new block is linked to the previous one via cryptographic hashes, forming an immutable sequence. A defining property is that once recorded and confirmed by the network, data cannot be easily altered retroactively, since any

attempt to tamper with a block would be evident to all participants because the hashes would mismatch. Blockchains are maintained by a consensus mechanism rather than a central authority, making them resilient and trust minimized. In essence, a blockchain acts as a “single source of truth” shared among parties who may not fully trust each other, ensuring data integrity and consistency across the board [10].

Smart Contracts: Smart contracts are self-executing programs stored on the blockchain that automatically execute predefined actions when certain conditions are met. They were popularised by platforms like Ethereum [11]. In simple terms, a smart contract is like a digital agreement whose terms are enforced by code: once deployed, its logic runs on the blockchain network without requiring external intervention. For example, a smart contract in healthcare could represent a patient’s consent directive. When a data access request is submitted, the contract verifies whether the patient has granted permission for that type of request, and either authorises access by generating a transaction on the ledger or denies it. As a result, smart contracts enable the automation of processes and the enforcement of regulations in a multiparty environment with ease. They are "self-executing contracts with the terms of agreement directly written into code," meaning that once they are carried out, they cannot be undone.

Consensus Mechanisms: In distributed ledgers, a consensus mechanism is the protocol that network nodes use to agree on the validity and order of transactions, thereby maintaining a consistent ledger state. Different blockchains use different algorithms: for example, Bitcoin’s consensus is Proof of Work (PoW), where nodes solve cryptographic puzzles to propose the next block; other networks use Proof of Stake (PoS), where nodes stake cryptocurrency, and the protocol randomly selects validators in proportion to their stake. In permissioned or consortium blockchains, where participants are known, Practical Byzantine Fault Tolerance (PBFT) and Raft are often employed. PBFT tolerates Byzantine faults by allowing the system to operate correctly even if some nodes act maliciously, which is critical in adversarial environments. At the same time, Raft, designed for trusted settings, provides simplicity, leader election, and fast consistency when nodes fail only by crashing, not by acting maliciously [12].

GDPR: Introduced in 2018, the GDPR defines how personal data must be collected, stored, and shared within the EU, forming the legal backbone of data protection practices. GDPR sets strict requirements: personal health information is classified as sensitive data, demanding a high level of protection. Key principles include lawfulness, transparency, data minimisation, purpose limitation, and integrity/confidentiality. Under GDPR, processing of health data generally requires the data subject’s explicit consent or another specific legal basis, and individuals have

rights to access their data, correct errors, and even request erasure (the “right to be forgotten”) [6].

EHDS: The EHDS is a recent EU regulatory initiative (formally adopted in 2025) aimed at creating a unified ecosystem for health data exchange across Europe. It establishes both primary (direct care) and secondary (research, policy, innovation) use frameworks for health data. Under EHDS, citizens should be able to access their electronic health records across member states and share them with healthcare providers as needed via the MyHealth@EU network. It also establishes the European Electronic Health Record Exchange Format (EHRxF) and interoperability standards that all certified Electronic Health Record (EHR) systems must follow. A core principle of EHDS is patient empowerment: patients have enhanced rights to obtain a copy of their data, to have it transmitted to another provider, to request corrections, and even to restrict access to parts of their record [4].

Electronic Identification, Authentication and Trust Services (eIDAS) [13]: eIDAS is an EU regulation that provides a framework for cross-border recognition of electronic IDs and trust services (e.g. electronic signatures, seals, timestamps, and certificates). Initially enacted in 2014 and updated in 2022 (often referred to as eIDAS 2.0), it seeks to ensure that an EU citizen or resident can use their national digital identity to authenticate themselves in any member state with the same legal validity as a local ID. For instance, a German citizen could identify themselves electronically to access a healthcare service in France, and the French system would trust the German e-ID as if it were a French one. Recently, eIDAS has introduced the concept of a European Digital Identity Wallet – a personal digital wallet for citizens to store and share identity credentials (e.g. ID cards, driving licenses, health insurance info, professional qualifications) in a secure, user-controlled manner.

CHAPTER 2

Literature Review

2.1. PRISMA Methodology

A systematic literature review was made using Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology [14]. The selection of studies included in this review, within the scope of this research, focused on works that address the application of blockchain technology to the secure, traceable management of healthcare data, with particular emphasis on digital chain-of-custody mechanisms and access control frameworks in regulated contexts such as the EU. The search was made using the following string:

blockchain AND ("healthcare data" OR "medical records" OR "health information") AND ("European Union" OR "EU regulation" OR gdpr OR ehds) AND (interoperability OR "data exchange" OR "cross-border")

The string was used to identify a total of 184 documents on the following websites:

- Scopus.
- Web of Science.
- ACM Digital Library.
- IEEE Xplore.

Out of the initial 184 documents identified, 19 were retrieved from Scopus, 11 from Web of Science, 83 from the ACM Digital Library, and 71 from IEEE Xplore. During the screening process, 15 duplicate records were identified and removed. Additionally, to reduce temporal bias and ensure regulatory relevance, the formal search was restricted to publications from 2023 onwards, when the literature already reflects the mature implementation of GDPR and explicitly engages with the emerging EHDS framework. This action removed 72 documents. From the remaining 91, 17 were removed due to a lack of full access.

Following the initial screening, 74 documents were considered potentially eligible for review. However, after a more detailed evaluation, only 13 were retained. Specifically, 31 papers were excluded based on their titles, which indicated they were outside the research scope. An additional 27 were removed after abstract screening because they did not address the study's core themes. The remaining three were excluded after full-text review because their content was found to be redundant with information already covered by the selected 13 documents.

The system illustrated in Figure 1 provides a more precise explanation of the process described.

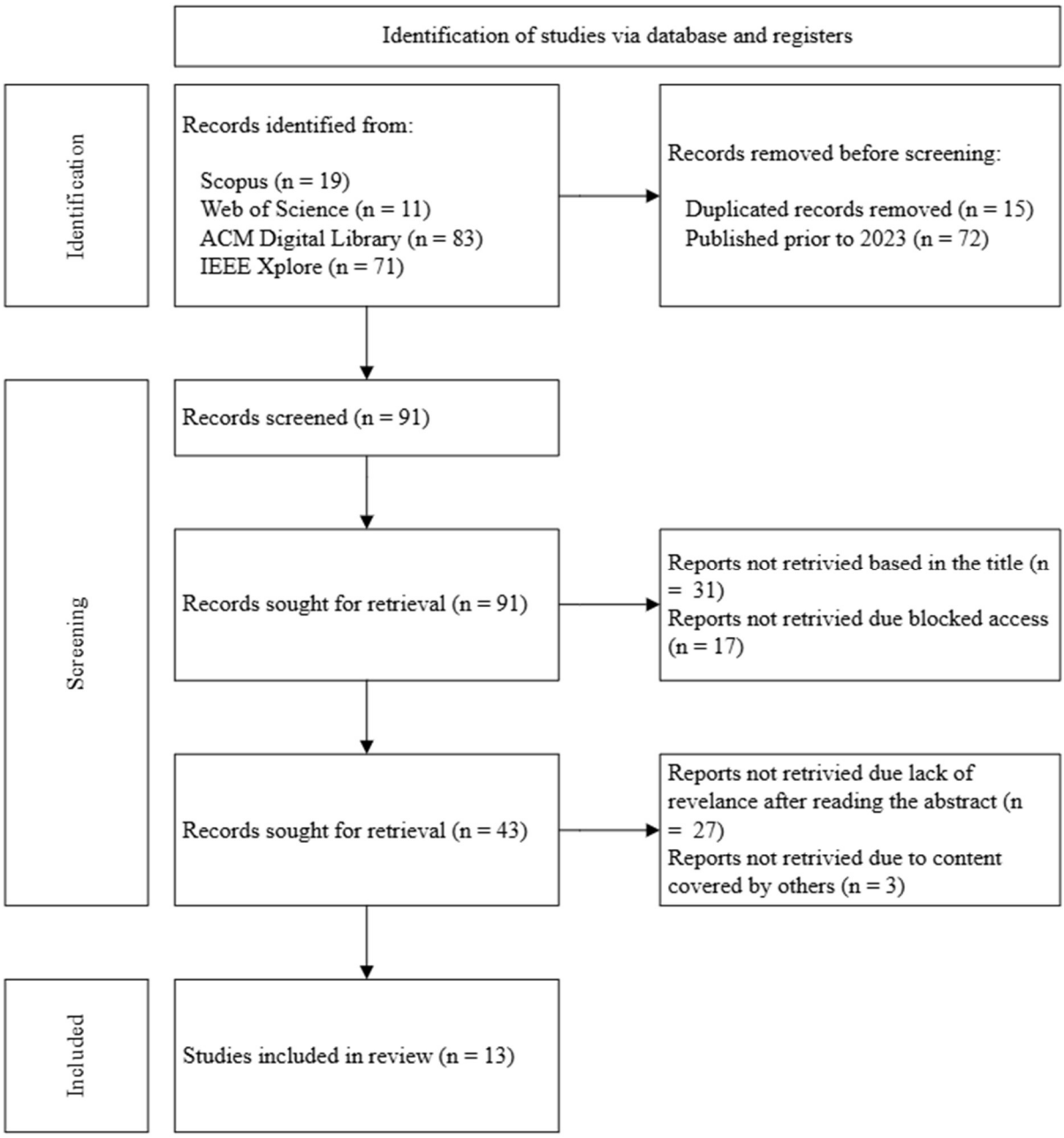


Figure 1 - PRISMA instance of the literature review

2.2. Literature Review

The literature on blockchain applications in healthcare has shown a steady growth over the past few years, reflecting increased academic and institutional interest in the topic. Illustrated in Figure 2 are the documents collected before any screening was applied. As can be observed, the number of publications has increased significantly from 2020 onwards, with a particularly notable concentration in the years 2023 and 2024.

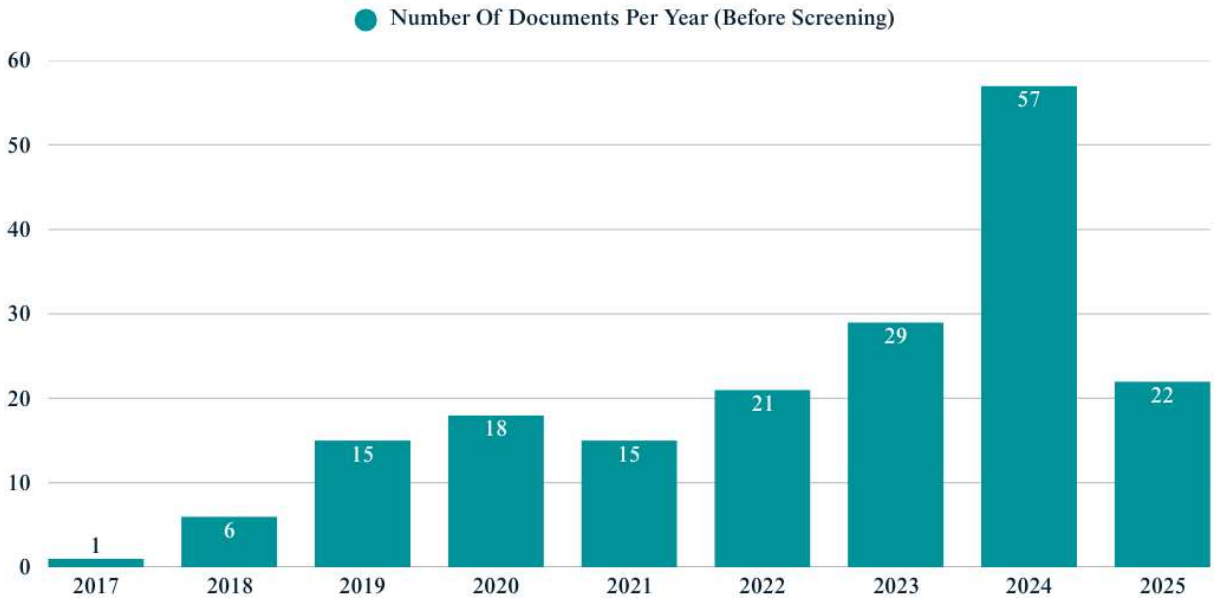


Figure 2 - Number of documents before screening

After the screening process was completed, the following documents in Table 1 were obtained.

Table 1 - Summary of documents

Title	Year	Summary
Blockchain-Based Service-Oriented Architecture for Consent Management, Access Control, and Auditing [8]	2023	This article proposes a service-oriented architecture (SOA) using blockchain for healthcare systems, enabling dynamic patient consent management, fine-grained access control, and immutable audit trails. The solution is designed to comply with GDPR and support interoperability between diverse healthcare information systems across organisations.
Significance of Blockchain Technology in the Healthcare Sector [18]	2023	Reviews technological strategies for achieving interoperability in healthcare, including semantic data alignment, API standardisation, and distributed system architectures. Though not blockchain-specific, the article provides essential context for integrating blockchain with existing IT systems.
A Comprehensive Study on the Application of Blockchain Technology's Use in Healthcare [19]	2023	This article examines how system-level security services can be applied to protect healthcare applications, particularly those that handle sensitive patient data. Topics include secure authentication, privacy-aware service design, and integration with privacy-enhancing technologies like blockchain.
Sec-Health: A Blockchain-Based Protocol for Securing Health Records [9]	2023	Investigates the role of blockchain in managing and protecting sensitive personal data across digital environments. It discusses smart contracts, cryptographic hashing, and decentralised access control, with a focus on medical and legal use cases where auditability is critical.

Blockchain-Based Healthcare Outcome Improvement: A Decentralized Method of Patient Care [15]	2024	Focuses on improving patient outcomes by applying blockchain to decentralise and standardise medical record exchange. The article highlights how real-time access to verified health information can reduce redundancy, prevent clinical errors, and improve data transparency in care pathways.
Empowering Healthcare: Hyperledger Blockchain for Unified Electronic Health Records and Organ Donation Integrity [16]	2024	Explores how hybrid encryption methods can be embedded within blockchain frameworks to secure sensitive healthcare data. It discusses the implementation of symmetric and asymmetric encryption combined with blockchain to protect data confidentiality during transmission and storage.
Leveraging Blockchain Technology for Secure and Efficient Storage of Medical Data [17]	2024	Presents a blockchain-based approach to medical data storage that ensures integrity, confidentiality, and availability. The system uses decentralised file management and cryptographic verification to prevent data tampering and unauthorised access, thereby enhancing the reliability of healthcare data management.
Towards Enhanced Data Integrity and Accountability: Leveraging Blockchain Technology in Healthcare [21]	2024	PETRA conference paper introducing an EHR architecture using blockchain to ensure data integrity, accountability, and secure logging in Healthcare 4.0 systems.
Unified Blockchain-Based Electronic Dental Record Ecosystem for Secure Data Exchange [22]	2024	Proposes a blockchain-enabled system for managing electronic dental records across institutions. It enables secure multi-party access, traceability, and patient control over data, while providing a scalable model applicable to other healthcare sectors. The system architecture includes smart contracts for access control and tamper-proof logging.
BlockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems [2]	2025	Introduces a blockchain-based cybersecurity framework tailored for electronic medical records that addresses challenges in secure data access, interoperability, and patient privacy. The system is designed to align with GDPR standards and provides layered security mechanisms, including hashing, encryption, and blockchain-based integrity verification.
Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: A quantitative analysis of ISO standards, GDPR, and HIPAA in blockchain technology [1]	2025	This empirical study analyses the perceived effectiveness of existing governance frameworks (GDPR, HIPAA, ISO) in supporting blockchain-based medical data exchange. It uses a quantitative model to evaluate dimensions such as confidentiality, availability, integrity, consent management, and regulatory compliance, identifying gaps and recommending governance improvements.
Blockchain Based Health Insurance System [20]	2025	Explores how distributed ledger technologies can support interoperability in healthcare by enabling secure multi-stakeholder data exchange. It outlines a reference model for linking disparate health data sources while maintaining data ownership and regulatory compliance.
Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records [3]	2025	Presents a smart-contract-based policy access control for EHRs on Ethereum, enabling dynamic consent, revocation, and GDPR compliance.

Following the initial analysis of the collected documents, as presented in Table 1, the literature was organised into two main thematic groups: Blockchain and Healthcare. This categorisation was established to reflect the dual focus of the thesis, which aims to assess the feasibility of a blockchain-based system for cross-border healthcare data management in the European Union. Given the subject's interdisciplinary nature, it was necessary to separate the analysis into two domains to ensure that both the technological and healthcare-specific dimensions are critically examined.

The Blockchain group includes documents that primarily address the technical aspects of blockchain technology, such as consensus mechanisms, clever contract design, data immutability, and system architectures. These works provide the foundational understanding necessary to evaluate how blockchain can support secure, decentralised, and auditable data exchange systems. The documents assigned to this group are: [9], [2], [8], [15] and [3].

On the other hand, the Healthcare group consists of documents that primarily engage with the context, needs, and constraints of healthcare systems, including patient data governance, interoperability challenges, consent management, and regulatory compliance. These sources are essential for understanding the practical requirements and barriers that a blockchain-based healthcare solution must address. Works in this category: [1], [16], [17], [18], [19], [20] and [21].

2.2.1. Blockchain

Da Costa et al. [9] propose Sec-Health, a blockchain-based protocol that fulfils key security requirements defined by health data regulations: confidentiality, fine-grained access control, data integrity, access revocation, and patient identity anonymity. Complementary needs, such as emergency access to records and system interoperability, are also addressed in their design, reflecting regulatory mandates (e.g., the GDPR in the EU) that demand both privacy and the timely availability of data in care emergencies [9]. By using a consortium blockchain and smart contracts, Sec-Health provides a trustworthy sharing mechanism for health records. The authors report that their prototype not only upholds security under various attack scenarios but also improves performance (reducing record access time and client-side overhead) compared to prior solutions [9]. This suggests that blockchain, when carefully engineered, can meet healthcare's strict security standards without unacceptable efficiency trade-offs.

The study by Pokharel et al. [2] focuses specifically on blockchain applications in healthcare, particularly in health monitoring. The authors identify and analyse blockchain-based frameworks designed to enhance data security, privacy, and interoperability in remote

patient monitoring systems. The paper highlights how blockchain can enable real-time data sharing between patients and healthcare providers while ensuring data integrity and access controls. A key contribution of the study is its classification of blockchain implementations based on parameters such as consensus mechanisms, data storage strategies, and integration with Internet of Things (IoT) devices. By narrowing its scope to healthcare-specific applications, the review offers a targeted evaluation of blockchain's role in improving digital health infrastructure, particularly in settings where continuous and trustworthy data flow is essential.

Román-Martínez et al. [8] aims to develop a service-oriented architecture backed by blockchain to manage patient consent across healthcare providers. In their framework, patients' consent directives (for who can access their data and for what purpose) are stored immutably on a blockchain. Smart contracts and fine-grained access control policies ensure that each data request is checked against the patient's consent. All access events are logged on the ledger for auditing by regulators or the patients themselves, enabling verification that healthcare providers comply with GDPR and the patient's wishes [8]. This approach addresses a critical challenge in cross-organisational health data exchange: ensuring data usage policies are enforced in a trustworthy manner. By adopting established health data standards (e.g., HL7 FHIR [22]) for data exchange, the system also maintains interoperability with existing EHR systems while using blockchain to provide a shared source of truth for consent and access events [8].

Namitha et al. [15] describes a blockchain-based health insurance system that automates claims submission, verification, and reimbursement via Ethereum smart contracts. Their design uses a multi-layer architecture: a blockchain layer with smart contracts for policy management, claims approval, and fraud detection; a decentralised storage layer for tamper-proof document storage; and a payment layer for disbursing payouts. By integrating middleware Application Programming Interfaces (API), the system achieves interoperability among hospitals, insurers, and patients, enabling real-time tracking of claims and ensuring compliance with regulatory requirements [15]. This demonstrates blockchain's ability to streamline multi-party processes: claims that once took weeks and extensive paperwork can now be settled faster, with transparent rules and audit trails. Moreover, the shared ledger helps reduce fraud and overhead by eliminating unnecessary intermediaries [15].

From a technical standpoint, permissioned blockchain frameworks (such as Hyperledger Fabric [23]) are often favoured in healthcare over public blockchains due to the need for access control and privacy [3]. For example, a policy-based access control (PBAC) system by Yaqub et al. [3] uses a permissionless Ethereum blockchain but carefully restricts data access via smart

contracts enforcing organisational policies. In their design, roles defined by GDPR (data subject, controller, requester) are embedded in access policies, and the blockchain logs who currently has permission to view or update a patient's record [3]. Patients can dynamically grant or revoke access and even audit the access history through the ledger. This blockchain-backed PBAC approach illustrates how decentralised trust can be combined with granular access rules to prevent unauthorised access while still enabling data sharing when appropriate. Transparency is enhanced, as patients and authorities gain visibility into data flows, while privacy is preserved by allowing only authorised reads/writes, as determined by smart-contract policy checks [3].

2.2.2. Healthcare

The work of Ahmed et al. [1] presents a comprehensive systematic literature review of blockchain-based applications across multiple domains, including finance, supply chain, healthcare, and energy. Although healthcare is only one of the sectors addressed, the paper provides valuable insights into overarching blockchain trends, architectural patterns, and open research challenges, including scalability, interoperability, and regulatory compliance. The authors classify blockchain use cases based on factors such as data sensitivity, trust models, and transaction volume, offering a framework to inform the evaluation of blockchain applicability in sensitive environments, such as healthcare. The review emphasises the importance of hybrid architectures (on-chain/off-chain storage) and intelligent contract design.

The work of Verma et al. [16] proposes a blockchain-based framework that reimagines data governance by placing patients at the centre. Their system introduces fine-grained access control mechanisms that allow patients to determine who may access their health records, under what conditions, and for how long. Using smart contracts deployed on Hyperledger Fabric, the framework automates consent enforcement and logs all transactions in an immutable ledger, ensuring accountability and auditability. The authors emphasise that such decentralisation not only empowers patients but also builds trust among stakeholders by mitigating the risk of unauthorised access or data tampering.

Similarly, the architecture proposed by Pise et al. [17] provides a robust solution for protecting patient data integrity by leveraging the blockchain's immutable ledger. Their system facilitates secure EHR storage and access control via encryption and distributed consensus. The authors stress that the unchangeable nature of blockchain records ensures the authenticity of clinical information, a critical requirement in environments where incorrect data could lead to harmful medical decisions. Furthermore, they demonstrate how permissioned networks can

restrict access to certified healthcare providers, enabling both data confidentiality and rapid access in emergency scenarios.

A complementary approach by Rai et al. [18] leverages blockchain to manage organ donation records across multiple hospitals. Their patient-centric model ensures that individuals maintain control over their donation preferences and associated health information. By enabling patients to dynamically update their consent status and share it securely across institutions, the system enhances both autonomy and transparency.

As highlighted by Galaba et al. [19], current blockchain implementations risk becoming isolated silos themselves if interoperability is not designed into the architecture from the start. Their study emphasises the need to integrate standards such as HL7 FHIR to ensure that data recorded on-chain can be consistently interpreted and utilised across diverse healthcare systems.

To address this concern, Verma et al. [16] propose a modular blockchain architecture that serves as an interoperability layer. Their system supports data translation from multiple formats into a unified schema before writing to the blockchain, ensuring cross-platform compatibility. They also integrate middleware services to bridge legacy health systems with blockchain nodes, effectively acting as translators and synchronizers between the old and new infrastructures. The study underscores that semantic interoperability, the ability to exchange and meaningfully interpret information, must accompany technical solutions for blockchain to be viable in real-world healthcare environments.

In a related contribution, Koulianos et al. [20] evaluate the role of distributed ledger technologies in facilitating cross-border data sharing, particularly within the EU. They argue that beyond aligning formats and protocols, blockchain provides a shared trust infrastructure that can mediate data access between institutions that otherwise lack formal integration agreements. By establishing tamper-proof audit trails and automated access rules, a blockchain-based network can significantly reduce the administrative friction of cross-organisational collaboration, a feature especially relevant in scenarios such as patient referrals, second opinions, or joint research initiatives across member states.

Equally important are the regulatory constraints that shape how healthcare data can be processed and shared, particularly within the European Union. The General Data Protection Regulation (GDPR) imposes strict rules on the use of health data, including explicit consent, the right to erasure, and data minimisation. Nekkalapudi et al. [23] address these constraints by proposing a layered architecture in which personal health data are stored off-chain, while only metadata and access records are kept on-chain. This hybrid approach offers a viable

compromise that maintains blockchain's immutability while respecting GDPR's data deletion requirements.

Further exploring compliance mechanisms, Allan et al. [21] develop an innovative contract-based framework to enforce key GDPR principles, including consent, purpose limitation, and data minimisation. Their system prevents unauthorised access and logs all transactions with cryptographic verification. By embedding legal constraints directly into the technical infrastructure, the authors argue for a compliance-by-design approach that minimises reliance on external audits or enforcement mechanisms.

2.3. Blockchain in EU Healthcare: Real-World Use Cases

Although much of the literature on blockchain in healthcare is still conceptual, some real-world EU implementations offer valuable practical insights. Notable examples include Estonia's blockchain-secured health records and the Pan-European PharmaLedger project for supply chain transparency. These initiatives show how blockchain can enhance data integrity, patient trust, and interoperability in European healthcare.

2.3.1. Estonia: Nationwide Blockchain-Secured Health Records

Estonia pioneered the use of blockchain in a national health system by integrating it into the country's electronic health records infrastructure. Since 2016, the Estonian eHealth Authority and the local tech firm Guardtime have used a KSI blockchain to timestamp and log every access to or change in patient records [24], [25]. This provides an immutable audit trail, making it impossible to tamper with or cover up alterations in medical data and significantly deterring fraud [26]. Key stakeholders include the Estonian Ministry of Social Affairs (which oversees e-health), the state-run eHealth Foundation, and Guardtime, the technology partner. The system is fully implemented nationwide, securing over a billion health data events, and is considered a global first in healthcare blockchain deployment [26].

Notable outcomes include enhanced transparency and trust in the integrity of records; patients can be confident that any access to their data is transparently logged, and the ability to detect insider misuse of sensitive documents is strengthened. Following this success, Estonia also collaborated with Finland's Guardtime and others on VaccineGuard, a blockchain-based COVID-19 vaccination certificate. Issued via the national patient portal, this secure digital passport allowed Estonians (and pilot partners in Hungary and Iceland) to prove vaccination status across borders, while linking to vaccine supply chain data for safety monitoring. The

VaccineGuard platform connected public health authorities, hospitals, citizens and even pharmaceutical companies in a distributed network, sharing verified health credentials without a central database, and was aligned with the EU Digital COVID Certificate initiative.

2.3.2. Pan-European PharmaLedger: Trusted Medicine Supply Chains

Beyond individual countries, the EU has backed consortium projects to apply blockchain in healthcare. A notable example is PharmaLedger, a 29-member public–private consortium (including 10 major pharmaceutical companies, several hospitals, and patient organisations) launched with EU funding in 2020 [27], [28]. PharmaLedger aims to create a "Digital Trust Ecosystem" for the pharmaceutical supply chain and clinical trials. After three years of development, the consortium (now a Swiss-based non-profit association) delivered its first product: an electronic Product Information (ePI) solution. This system replaces the paper leaflets in medicine boxes with a blockchain-backed digital alternative, allowing patients to simply scan a drug's barcode with a smartphone to retrieve the up-to-date official leaflet and safety information. The blockchain ensures that the ePI data is authentic and traceable to the manufacturer, eliminating the risk of outdated or fraudulent drug information. The project's stakeholders span multiple countries and sectors: pharmaceutical firms (e.g. Novartis, GSK, Pfizer), healthcare providers, EU research agencies, and technology partners all collaborated, making it a multi-stakeholder EU-backed effort [28]. As of 2023, PharmaLedger's ePI is live and in use, and the consortium is expanding into other use cases – including blockchain systems for clinical trial data management (to improve data integrity and patient consent tracking across sites) and for medicine supply chain transparency (to authenticate products and prevent counterfeits).

A notable outcome has been the successful coordination of diverse players under a single framework. However, the initiative faced governance challenges: some companies departed due to differing priorities, underscoring the difficulty of aligning many competitors on a single platform [28]. Even so, PharmaLedger demonstrated that blockchain can be applied at scale in Europe's health sector, supported by public funding, yielding a functional solution that improves trust in healthcare information and potentially streamlines regulatory compliance across EU markets.

2.4. Critical Reflection and Positioning of This Research

The reviewed literature reveals a growing interest in blockchain's potential to support secure, decentralised, and auditable data management in healthcare. Most of the documents categorised under the Blockchain group emphasise foundational technologies, such as smart contracts, consensus algorithms, and permissioned networks, and explain how these can, in theory, support privacy, integrity, and transparency in data handling. Meanwhile, the Healthcare group focuses on specific use cases such as patient consent, data interoperability, and remote health monitoring, with several works presenting proof-of-concept implementations or small-scale pilots.

A clear trend across both groups is the fragmented and localised nature of the proposed solutions. Research efforts tend to focus on specific functionalities (e.g., access control or claims automation) or on national-level applications, without extending to cross-border interoperability or addressing the governance challenges of a European-wide health data infrastructure. While compliance with the GDPR and integration with existing e-health standards are often mentioned, they are rarely addressed holistically in system design.

In contrast, this thesis aims to build upon these existing technological and healthcare-specific foundations while proposing a comprehensive architecture tailored for cross-border healthcare data exchange within the EU. The goal is to move beyond isolated or country-specific initiatives by conceptualising a federated, blockchain-based framework that supports secure, auditable, and patient-controlled data sharing across member states. Emphasis is placed on decentralised consent management, auditability by design, and real-time access control, dimensions acknowledged in the literature but not yet fully operationalised at scale.

CHAPTER 3

Requirements & Architecture

3.1. DSRM Methodology

The European health-data landscape has grown increasingly complex: fragmented across Member States, reliant on heterogeneous providers and infrastructures, and constrained by stringent privacy safeguards. In parallel, the GDPR and the emerging EHDS framework heighten requirements for verifiable consent, data minimisation, and trustworthy audit, making it essential to adopt technological approaches that ensure reliable, continuous control and evidence throughout cross-border data-sharing episodes.

Accordingly, this chapter corresponds primarily to the design and development stage of the Design Science Research Methodology (DSRM), where the artefact is specified and architected. DSRM, as articulated by Peffers et al. (Figure 3), serves as a guiding structure for conceiving and developing an innovative artefact with practical relevance and scientific rigour, particularly suited to investigations that address real-world problems by creating purposeful technological solutions.

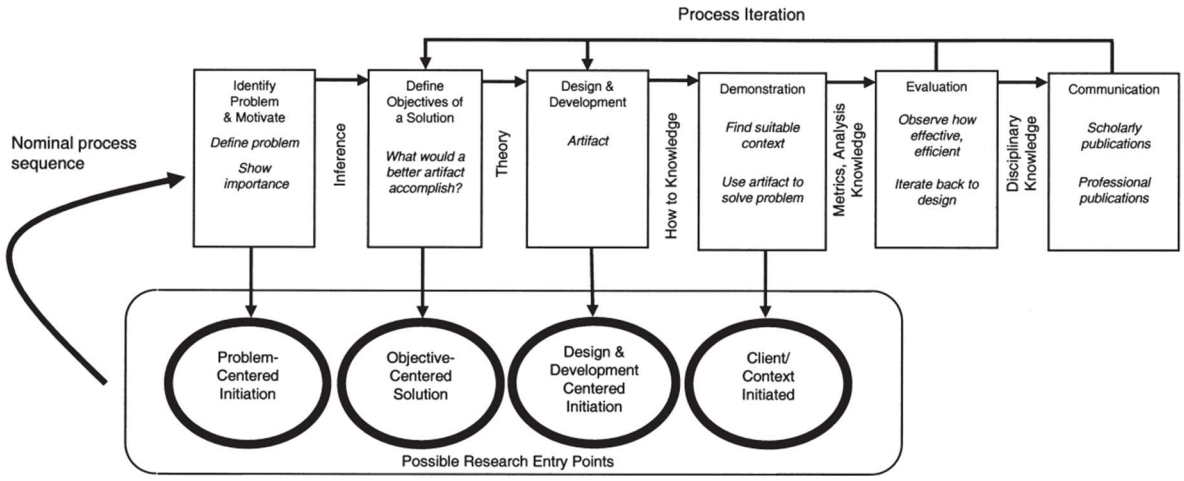


Figure 3 - Design Science Research Methodology (Peffers et al.)

3.2. Central Coordination Layer

The system's highest level consists of two sovereign healthcare contexts, Country A and Country B, each represented by a "provider" (hospital, clinic, lab, or other medical facility) that maintains and controls its patients' clinical records locally. A Central EU Coordination Blockchain, which serves as an impartial trust fabric, sits between them. Only the minimal, non-sensitive metadata needed for cross-border coordination, most notably consent tokens and audit events, is recorded by the central chain; medical content is not stored there.

A cross-border interaction involves at least four steps from an operational perspective. Initially, a provider in the country making the request indicates that they wish to view a specific portion of a patient's records held by a provider in the other nation. Second, the request is automatically compared to a legitimate consent token that has already been registered for that patient and scope on the central blockchain. Third, the chain returns a positive authorisation signal if a valid token is present within its time window and if not, authorisation fails deterministically. Fourth, a tamper-evident audit entry containing the request identifier, consent token reference, timestamps, and outcome is appended to the central ledger by both parties after the clinical data is transferred directly between providers via a secure, point-to-point channel outside the blockchain.

This EU-level locus, which controls the legality and traceability of exchanges between sovereign systems, is where cross-border interoperability, consent enforcement, and auditability converge. The central chain maintains national data sovereignty and privacy while providing verifiable proof of legal access by storing personal health-related data off-chain and recording only consent and audit metadata. Above all, it establishes system-level properties. Deterministic authorisation, revocation effectiveness, and immutable audit are examples of cross-jurisdictional practices that can be defined and assessed independently of diverse national implementations.

3.3. Participants

Participants are reduced to four key roles at the central coordination layer: patients (through their home context), EU Members (through national gateways), the EU (consortium and trust services), and an Independent Auditor. When combined, they allow cross-border coordination without adding personal health information to the ledger: patients create or withdraw consent, the EU guarantees trustworthy governance and trust anchors, Member States carry out operational writes (consent presence/withdrawal, authorisation requests, delivery receipts), and the auditor provides external assurance.

3.3.1. EU Members

Role: Only submit control events. Represent domestic healthcare ecosystems.

Central chain core actions include:

- Register or withdraw consent for cross-border use.

- For a specified scope and purpose, request a deterministic authorisation (Allow/Deny).
- To finish the audit trail, add delivery receipts following the off-chain transfer.

Example: For instance, a patient's consent for "prescription history to Hospital X (Member B), valid 30 days" is recorded by Member A's national gateway; Member B's gateway requests authorisation; upon "Allow," Member A verifies delivery with a receipt on the central chain.

3.3.2. EU (Consortium & Trust Services)

Role: Provide the neutral substrate, including trust anchors, governance, and permissioned consensus.

Central chain core actions include:

- Managing validator nodes and documenting changes to governance (versions, membership, and parameters).
- To ensure that authorisations and revocations have a clear legal impact, provide identity (eIDAS-recognised organisational credentials) and qualified timestamps.

Example: For instance, qualified timestamps seal all subsequent decisions and revocations with the new rule set when the consortium initiates a parameter update that reduces the maximum validity of consent.

3.3.3. Patients

Role: Individuals who create and revoke consent; review their own audit records.

Central chain core actions include:

- Publish (or revoke) consent presence via the home country's channel.
- Later, query subject-scoped evidence that demonstrates who had access to what, when, and for what legal reason.

Example: For instance, if a patient withdraws previously authorised access, any subsequent cross-border requests for that scope result in a Deny; the audit displays the cutoff and the denied attempts without disclosing any personal health information.

3.3.4. Auditor(s)

Role: Read-only, accredited assurance independent of enforcement.

Central chain core actions include:

- Obtain evidence bundles (consent lifecycle → decision → delivery/denial) to verify policy and control compliance.
- For ongoing assurance, examine governance records and availability/latency goals.

For instance, an auditor gathers evidence from a sample of cross-border incidents and verifies that no "Allow" was granted without active consent, that revocations occurred before further requests, and that audit trails are comprehensive and unalterable.

3.4. Functional Requirements

The proposed artefact uses a federated, permissioned blockchain design to operationalise cross-border interoperability without centralising protected health information (PHI). An EU-level meta-chain offers tamper-evident audit and cross-border consent verification, while national blockchains coordinate domestically. Verifiable accountability, data minimisation, and patient-centric control are all implemented in this configuration. Table 2 lists the prerequisites for this.

Table 2 - Functional Requirements

ID	Functional Requirement	Description
FR-01	Identity & Authentication	Verify the identities of patients and medical personnel and attach signatures to on-chain transactions.
FR-02	Provider Trust Registry	Keep a list of approved healthcare organisations and providers that can send and receive data internationally.
FR-03	Consent Request	Permit a requesting hospital to publish a consent request (duration, scope, and purpose) as a transaction that notifies patients.
FR-04	Patient Approval/Revocation	Give patients the option to approve or reject requests at any time. Decisions should be automatically enforced and recorded in an unchangeable manner.
FR-05	Cross-Border Consent Verification	Use national-chain records and EU-level references (hash/ID) to confirm consent status and scope before any foreign access.
FR-06	Authorisation at Data Holder	Before release, demand that the hospital holding the data verify the requester's identity, scope, validity window, and consent hash or ID.
FR-07	Emergency “Break-Glass”	Encourage emergency access under more stringent controls, requiring post-hoc justification and providing real-time alerts to patients and auditors.
FR-08	Immutable Audit & Views	Every request and decision should include tamper-evident logs, and patient and auditor views that demonstrate who accessed what, when, and why should be made public.
FR-09	National ↔ EU Ledger Sync	To facilitate cross-border verification, publish minimal, non-sensitive fingerprints (such as consent IDs/hashes and access events) from national chains to the EU meta-chain.

FR-10	Standards-Based Exchange & Minimisation	Keep PHI off-chain and support standardised payloads (e.g., FHIR/EHRxF) over a secure channel, with on-chain metadata referencing them only when data is released.

3.5. Non-Functional Requirements

The non-functional envelope must prioritise privacy/compliance by design, verifiable accountability, and care-grade operability to balance cross-border clinical utility with the moral and legal restrictions of managing health data in Europe. GDPR exposure is reduced through permissioned consensus and off-chain PHI; accountability is operationalised through immutable, patient- and regulator-readable logs; the ledger is kept from becoming a new silo through standards-first interfaces; and point-of-care viability is ensured across Member States through explicit targets for latency, availability, and revocation propagation. Table 3 lists the prerequisites for this.

Table 3 - Non-Functional Requirements

ID	Non-Functional Requirement	Description
NFR-01	Security: Cryptography & Key Management	Enforce mutual TLS, hardware-backed key custody, and end-to-end cryptography (in transit and at rest) for organisational clients and validator nodes.
NFR-02	Privacy: Data Minimisation	To meet data minimisation requirements and enable off-chain erasure, ensure that no PHI is written to the chain and that only hashes, pointers, and policy metadata are stored.
NFR-03	Compliance: GDPR & EHDS Alignment	Comply with EHRxF profiles and EHDS cross-border exchange; exhibit lawfulness, purpose limitation, and data-subject rights.
NFR-04	Auditability & Non-Repudiation	Create audit trails for every consent/access event that are time-stamped, tamper-evident, and verifiable by patients and supervisory authorities.
NFR-05	Interoperability (Semantic & Syntactic)	To ensure the ledger maintains trust without becoming a data silo, expose standards-first interfaces (e.g., HL7 FHIR/EHRxF).
NFR-06	Performance: Consent Check Latency	Reach near real-time consent verification (e.g., sub-seconds to a few seconds across borders) that is appropriate for point-of-care workflows.
NFR-07	Availability & Resilience	Provide high service continuity (multi-AZ deployment, graceful degradation of non-critical services) for logging and verification.
NFR-08	Revocation Propagation	To prevent the execution of outdated permissions across borders, swiftly disseminate consent revocations and expirations across national and EU levels.

NFR-09	Maintainability & Upgradability	Provide backwards-compatible interfaces for safe contract/schema evolution, versioning, and rolling upgrades.
NFR-10	Governance & Onboarding	Establish clear procedures appropriate for a multi-state consortium for node admission, policy modifications, incident response, and service-level publication.

To clarify that the non-functional requirements in Table 3 are not defined ad hoc but derived from concrete European regulatory and policy instruments, Table 4 links each requirement identifier to its primary normative sources, particularly the GDPR, the EHDS framework and the eIDAS trust and identity ecosystem.

Table 4 - NFR Justification

ID	Justification / Source
NFR-01	GDPR Art. 5(1)(f) "integrity and confidentiality" and Art. 32 "security of processing" (encryption, resilience, technical and organisational measures) [6]. eIDAS Regulation for trusted time-stamps, signatures and secure trust services [13].
NFR-02	GDPR Art. 5(1)(c) data minimisation and Art. 5(1)(e) storage limitation; Art. 17 right to erasure; Art. 25 data protection by design and by default (minimised data, short retention, limited accessibility) [6].
NFR-03	GDPR Arts. 5–7 (lawfulness, consent, purpose limitation), Art. 9 (special categories, including health data) [6]. EHDS Regulation requirements for primary-use exchanges, MyHealth@EU and EHRxF-based cross-border EHR access [4], ensuring alignment with the emerging EU health-data framework.
NFR-04	GDPR Art. 5(2) accountability and Art. 30 records of processing activities (demonstrable compliance and traceability) [6]. EHDS governance and oversight provisions (auditability of cross-border flows) [4] and eIDAS qualified timestamps for evidential integrity [13].
NFR-05	EHDS requirements for interoperable formats and services (MyHealth@EU, EHRxF) as the reference for syntactic and semantic interoperability across Member States [4]; use of HL7 FHIR/EHRxF as the concrete standards profile.
NFR-06	EHDS's emphasis on timely, effective cross-border access to electronic health data for continuity of care [4] justifies explicit targets for consent-check latency suitable for point-of-care workflows.
NFR-07	GDPR Art. 32(1)(b) requiring the "ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services" [6]. EHDS expectations for robust, highly available EU-level health-data infrastructures [4].
NFR-08	GDPR Art. 7(3) right to withdraw consent at any time, Art. 17 right to erasure and Art. 21 right to object to processing, requiring revocation to be technically enforceable without undue delay [6].
NFR-09	GDPR Art. 25 data protection by design and by default (need for maintainable, upgradable controls that preserve safeguards over time) [6]. Data Protection Commission EHDS and EHRxF as evolving EU frameworks, implying versioning and backwards-compatible evolution of interfaces [4].

NFR-10	GDPR Art. 5(2) accountability and Arts. 24 and 26 on controller responsibilities and joint controllership (transparent allocation of roles, policies and incident handling) [6]. EHDS consortium-level governance requirements [4] and the eIDAS regime for trusted identity, signatures and timestamps in multi-party infrastructures [13].

3.6. EU Central Blockchain Architecture

The central EU coordination blockchain can be described as a four-layer stack that narrows the system to authorisation and audit while keeping clinical content off-chain. At the foundation, the platform and consensus layer provide a permissioned, geo-distributed ledger with Byzantine-fault-tolerant finality, deterministic ordering, qualified timestamps and mutually authenticated links between accredited nodes. This tier establishes availability, trusted time and cryptographic integrity without persisting any medical data.

Above it, the identity and ledger core assigns pseudonymous handles to subjects and providers, maintains consortium membership and attestation using eIDAS-recognised organisational credentials, and records only minimised metadata, references to consent tokens, signed access intents, authorisation decisions, and audit events, ensuring that personal health information is always kept outside the chain. Each decision is time-stamped, signed, and anchored as an immutable audit event. Evidence bundles (inclusion proofs, decision signatures, and time attestations) enable patient transparency and supervisory oversight. The authorisation and audit services layer builds upon this foundation by evaluating each access intent deterministically against membership status, consent scope and purpose, validity windows and revocation or expiry, and, where policy permits, a narrowly bounded emergency path.

The message flows that link countries and facilities to the central chain are defined at the perimeter by the bridge and transparency layer. These flows include publishing or revoking consent references, submitting access intents, receiving allow or deny decisions, notifying off-chain delivery, enforcing replay protection via nonces and expiry windows, and supporting both ledger-enabled participants, who provide lightweight proofs from national systems and legacy participants who use an EU access gateway.

The architecture described is further explained in Figure 4.

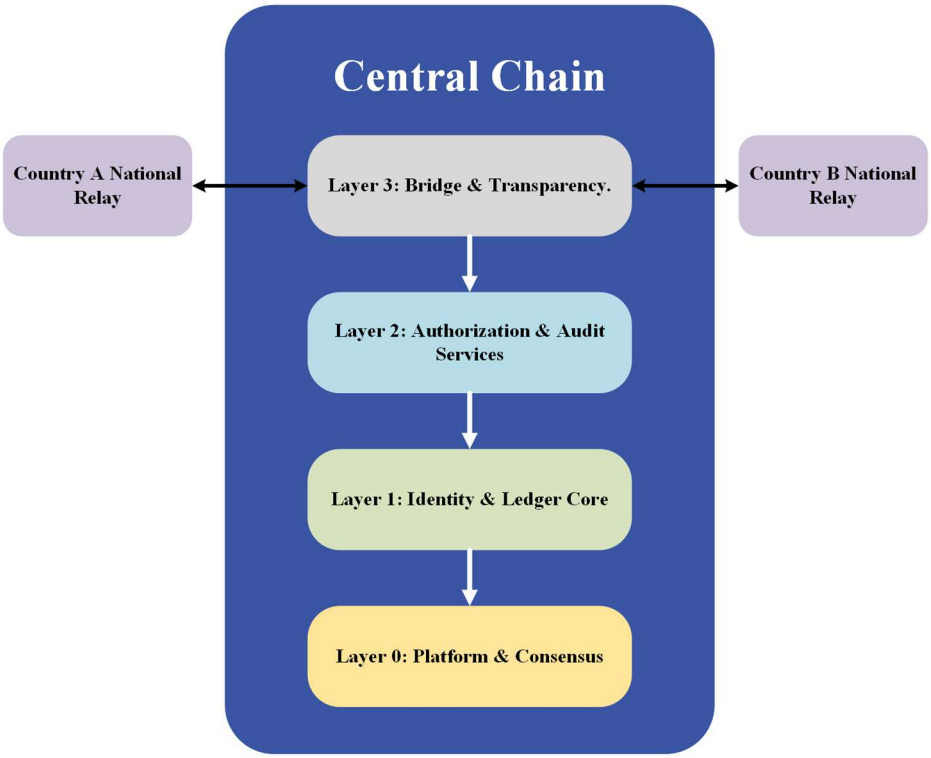


Figure 4 - Central Chain

The four layers can be summed up as follows:

- **Layer 0 - Platform and Consensus**: Provides a geo-distributed, permissioned ledger with mutual TLS, qualified timestamps, deterministic ordering, and validator keys supported by HSMs, which offer cryptographic integrity and availability without storing clinical data.
- **Layer 1 - Identity and Ledger Core**: Keeps minimal on-chain metadata (such as consent-token references, signed intents, and audit events), pseudonymous handles for subjects and providers, and eIDAS-recognised membership guarantees that PHI stays completely off-chain.
- **Layer 2 - Authorisation and Audit Services**: Evaluates access intents deterministically, considering emergency routes and revocation. A signed, time-qualified audit event supports every choice. Evidence bundles promote regulatory oversight and subject transparency.
- **Layer 3 - Bridge and Transparency**: Sets up perimeter message flows (such as PublishConsent and AccessIntent), protects them with nonces and expiration windows, and allows both national-ledger participants and legacy actors to use an EU relay. Enables audit roles to see things in read-only mode.

3.7. Smart contracts

Since smart contracts are the precise location where abstract legal and policy requirements are translated into enforceable, machine-verifiable behaviour on the Central EU Coordination Blockchain, they merit special attention in this thesis. Clinical content remains off-chain under national sovereignty, while the central layer manages consent, authorisation, and audit. Thus far, the architecture has established the fundamental separation of concerns. The rules governing these coordination tasks must be consistent, deterministic, and independently verifiable by all participating jurisdictions for that separation to produce reliable cross-border exchange. That is precisely what smart contracts do: they replace implicit trust and bilateral agreements with transparent, repeatable results by encoding the admissible actions, preconditions, and consequences as tamper-resistant logic that is executed identically across all validating nodes.

In the health sector, where the legal foundation for processing is dynamic and conditional, this need is exceptionally pressing. Consent may be given for a limited period, limited to a specific episode of care, abruptly revoked, or temporarily circumvented in an emergency. Cross-border assurance and post-hoc accountability are made more difficult in traditional systems because those details are handled in application code and organisational procedures that differ by nation and provider. No authorisation can be generated without a corresponding, legitimate on-chain ground, thanks to smart contracts that enable the central layer to capture these subtleties as first-class states transition through creation, amendment, revocation, expiration, and emergency override.

From a compliance standpoint, smart contracts shift the burden of proof from institutional assertions to cryptographic evidence. Because contract execution and outcomes are recorded immutably with trusted time and total ordering, each authorisation decision can be accompanied by an auditable proof that the pre-conditions held at that moment. This directly supports the accountability principle and turns obligations into testable properties for evaluation: for example, that no “allow” decision can occur after a revocation takes effect, or that emergency access is both narrowly scoped and followed by post-hoc justification. In other words, smart contracts do not just implement policy, they evidence it in a form that patients, providers, and supervisory authorities can verify independently.

The central chain should only contain hashes, event metadata, and pseudonymous identifiers. This work avoids explicitly centralising personal health information. Such a "thin" ledger would be little more than a passive log in the absence of smart contracts. The duplicate

minimal records become active guarantees with contracts: an audit append is an obligation that completes the evidentiary chain for a particular episode, rather than a best-effort write; a revocation event is a state change that deterministically invalidates future requests rather than an annotation, and a consent token handle is a condition that the authorisation logic must satisfy. Thus, a privacy-preserving design is given operational force by smart contracts.

Bridges emphasise the need for contract-based coordination even more. The system must accept intents and attestations from diverse environments. While some nations will rely on an EU access gateway serving as a proxy, others will present light proofs derived from national ledgers. Smart contracts provide the neutral point where disparate assurance paths converge and are assessed under a single, published ruleset. The audit trail's shape, the authorisation's semantics, and the acceptance requirements can all change, but the bridge itself cannot. The smart contracts required for the Central Chain to adhere to all previously discussed requirements are listed in Table 5.

Table 5 - Smart Contracts

Smart Contracts	Operation
Membership & Roles Registry	Participants and their roles (requester, data holder, supervisor/regulator, national relay, EU gateway) can be admitted, updated, or suspended.
Provider Trust Register	Register and update the identities of recognised healthcare providers (institutions and, if relevant, licensed professionals).
Consent Token Registry	Cross-border valid consent tokens can be created, narrowed (amended), revoked, and expired.
Authorization Oracle	Determine whether to grant or deny access requests based on membership status and consent status.
Emergency Access Controller	Permit limited emergency access under specified circumstances, subject to obligations (notifications, post-hoc justification).
Cross-Border Audit & Evidence Ledger	Add unchangeable lifecycle and access events; put together bundles of verifiable evidence for supervision.
Time & Ordering Authority	To ensure revocation effectiveness, tie decisions and lifecycle modifications to trusted time and ledger order.
Governance & Parameters	Membership rules, scope/purpose code sets, consent TTLs, and upgrades are examples of network/policy changes that can be proposed, voted on, and implemented.
Observability & Transparency Interface	Give subjects, providers, supervisors, and regulators role-appropriate reporting and querying.

CHAPTER 4

Evaluation

4.1. Evaluation Approach

The purpose of the artefact's demonstration and evaluation within the Design Science Research Methodology (DSRM) is to ascertain the extent to which the proposed central coordination layer meets the specified requirements. It adds value in its intended context: cross-border, EU-wide health data exchange. Rather than empirical testing or simulation, the evaluation takes a document-based, argumentative approach grounded in legal frameworks and architectural design invariants, given the theoretical nature of the work. The review is organised around three complementary lenses: regulatory compliance, auditability and oversight, and privacy by design and proportionality, to ensure analytical coverage and depth. The fundamental responsibilities of any cross-border coordination mechanism functioning under European law are reflected in these lenses.

4.1.1. Regulatory Compliance

The General Data Protection Regulation (GDPR), the European Health Data Space (EHDS), and the eIDAS regulation are three necessary European legal instruments that this lens evaluates the artefact's compliance with throughout the entire consent and access lifecycle. The analysis examines how the architecture protects data-subject rights such as withdrawal, transparency, and auditability, enforces purpose limitation, and operationalises a legitimate legal basis for data exchange.

The assessment is carried out by mapping architectural components to specific legal requirements (e.g., GDPR Art. 6, 7, 13, and 25), such as consent token issuance, time-bounded revocation, pseudonymous identifiers, and role-based access. For example, qualified timestamps and deterministic revocation semantics are used to enforce consent withdrawal, making any further access attempts inexecutable. While identity assurance and accountability are supported by eIDAS-compliant organisational credentials and mutual TLS between nodes, purpose limitation and data minimisation are accomplished by encoding access intents using pre-defined code sets.

The result is a reasoned conformity assessment: any residual assumptions (such as off-chain identity management) are made explicit and scoped, and the artefact satisfies the main requirements of lawful processing, consent governance, and organisational authentication.

4.1.2. Audit, Evidence, and Oversight

This dimension concerns accountability, specifically whether the artefact can produce irrefutable, verifiable proof for each cross-border exchange. Although the data itself is still off-chain, the evaluation focuses on the traceability of the consent lifecycle, access decisions, and clinical data transmission. The architecture records tamper-evident events at every step of the process, each of which includes a cryptographic signature, a qualified timestamp, and a link to the event that preceded it in the flow.

Significantly, read access to these logs is role-bound, meaning that interactions in a transparency interface can be examined by patients, auditors, and supervisory authorities without exposing clinical content or escalating privileges. According to the evaluation's findings, the system satisfies the fundamental requirements for auditability and oversight under GDPR Art. 30 and Recital 74, as well as the governance transparency requirements expected under EHDS.

4.1.3. Privacy by Design and Proportionality

The architecture's compliance with the GDPR Art. 5 and Art. 25 principles of data minimisation, unlinkability, and necessity is the subject of the third analytical lens. The fundamental design principle is that the coordination layer processes only pseudonymous metadata (such as hashed consent tokens and scoped access intents) and never stores clinical content on-chain.

The evaluation argues that the artefact embodies privacy by design across multiple dimensions. Pseudonymous identifiers prevent identity linkage without off-chain correlation. To ensure consistency and minimise semantic leakage, all access requests and consents are encoded in controlled vocabularies. Revocations are handled deterministically, and emergency access is limited and documented. The chain only records the data required to establish and demonstrate lawfulness, maintaining proportionality.

As a result, the coordination layer remains fully functional within its intended scope while avoiding excessive processing and mitigating metadata risks. Without violating national data sovereignty or going beyond the necessity principle, it promotes cross-border interoperability.

4.2. Use Cases

The theoretical assessment of the central coordination layer is organised around specific cross-border episodes that the artefact must support. Without assuming implementation or empirical

testing, each case isolates a legally and operationally significant moment, registers an access intent, issues a deterministic authorisation, audits the entire episode, invokes a narrowly scoped emergency path, and enforces revocation. When taken as a whole, they provide a foundation for evaluating proportionality, privacy by design, auditability and oversight, and regulatory compliance. The purpose, actors, preconditions, main flow, postconditions/evidence, and evaluation claims are all presented consistently across the cases, neatly aligning with the thesis requirements and facilitating a consistent, document-based assessment.

4.2.1. Use Case 1: Register the Request

When a provider in Member State B seeks access to a specific subset of a patient's records in Member State A, a cross-border episode begins. The national gateway in B logs the intent as a pre-access event on the central coordination layer before any clinical content moves. When determining how to move forward off-chain, Member State A can refer to a precise, unchangeable statement of intent thanks to this anchoring fix's goal and scope, under trusted time and deterministic ordering. Because an auditor or supervisor can subsequently confirm that access was preceded by a declared purpose and scope rather than being implied or inferred, the act of registration, by design, carries only minimal metadata and no health-related personal data, yet it already advances accountability.

Success criteria

- The access intent is anchored on the central ledger before any off-chain transfer.
- The intent contains only minimal, non-identifying metadata.
- The intent is bound to trusted time and ordering.

Verifiable properties

- Every later decision for the same episode references an earlier intent (causality).
- The intent record carries a qualified timestamp and an inclusion proof in the ledger history.
- The intent is attributable to an admitted organisational identity (eIDAS-recognised certificate).

The flow of the use case is demonstrated in Figure 5.

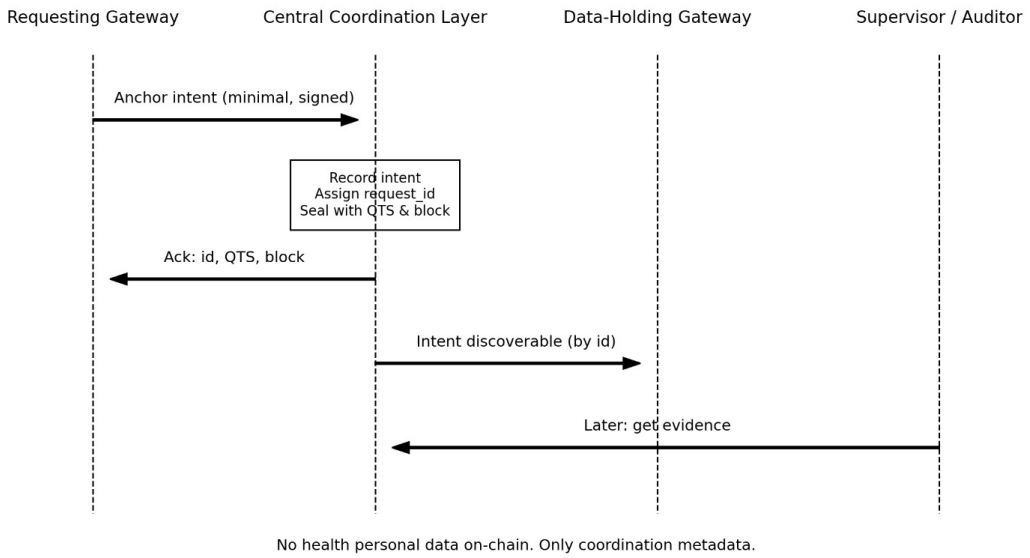


Figure 5 - Use case 1 Diagram example of communication

4.2.2. Use Case 2: Accepting the request

The requester's current membership status and the existence of an active, scope-matching consent token for the data subject are the two pillars against which the central layer assesses the intent after it has been anchored. The chain returns a "Allow" decision if both conditions hold within their respective validity windows, if not, the result is a definitive "Deny." Qualified time seals the decision and incorporates it into the unchangeable episode story. The ledger documents that a legitimate basis existed (or did not) at a specific moment, traceable to the prior intent, rather than exposing or storing clinical data on the chain. This creates a clear path from the stated purpose to the authorisation outcome, allowing later confirmation that decisions were made without relying on opaque, off-ledger assumptions and that no authorisation was granted without a legitimate legal basis.

Success criteria

- Allow occurs only if an active, scope-matching consent is present within its validity window and the requester holds an active role.
- Deny occurs deterministically otherwise (absent/mismatched/expired consent; suspended requester).
- The decision itself does not disclose personal data.

Verifiable properties

- For any decision, there exists either contemporaneous consent that satisfies scope, purpose, and time, or a recorded absence leading to Deny.

- Each decision carries a qualified timestamp, block reference, and signer traceable to an admitted organisation.
- Decision outcomes are reproducible from on-chain state at that height.

The flow of the use case is demonstrated in Figure 6.

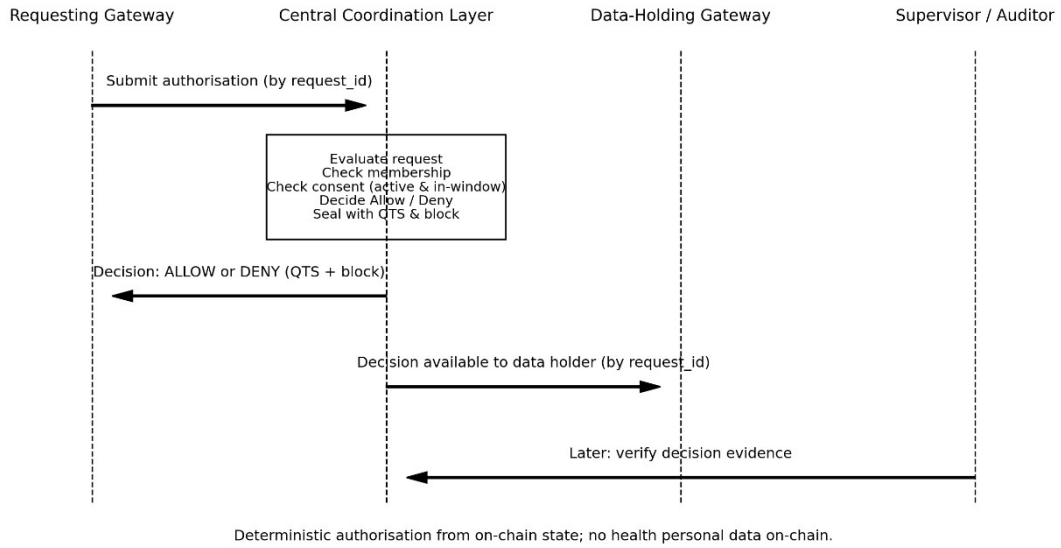


Figure 6 - Use case 2 Diagram example of communication

4.2.3. Use Case 3: Auditing the request

The central layer provides a logical, tamper-evident account of the entire event, including the authorisation outcome and, if applicable, the bilateral, off-chain transfer and its delivery receipt. By examining the intent anchor, the authorisation decision, the related consent lifecycle entries, and the final delivery or denial marker, all connected by correlation and safeguarded by inclusion proofs and qualified timestamps, a subject, a regulator, or an independent auditor can piece together what transpired. Transparency for oversight is achieved without disclosing personal health information because very little metadata is recorded. The resulting evidence bundle is sufficient to address the following supervision-related questions: who made the request, why and to what extent, under what legal basis, when the decision was made, and whether a transfer was later declared.

Success criteria

- An authorised reader can reconstruct an episode end-to-end: intent → decision → delivery/denial → consent lifecycle references.
- Evidence is tamper-evident and can be exported without revealing personal data.

- Oversight access is role-bounded and logged.

Verifiable properties

- The episode has a complete set of immutable entries linked by a correlation identifier.
- Evidence bundles include inclusion proofs and qualified timestamps for each step.
- Read paths differ by role without privilege escalation.

The flow of the use case is demonstrated in Figure 7.

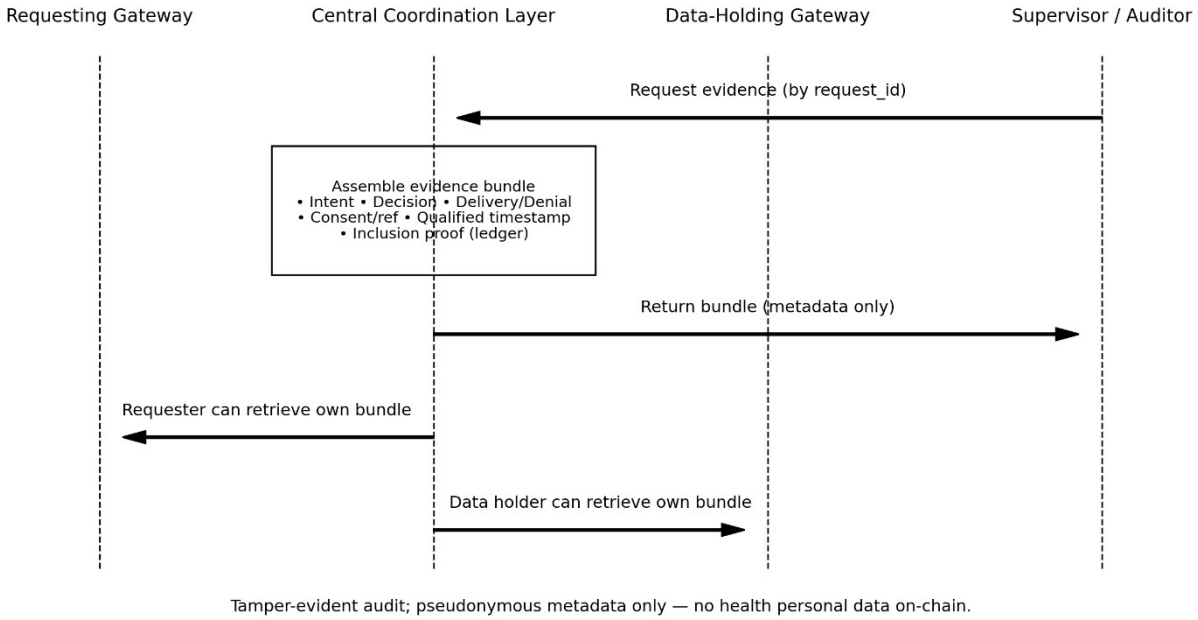


Figure 7 - Use case 3 Diagram example of communication

4.2.4. Use Case 4: Break-glass request

The requesting gateway records an emergency intent in extraordinary situations where prior consent is unavailable, and delay would put the patient in danger. Only minimum-necessary categories are eligible, additional preconditions apply, notifications and post-hoc justification are required, and the central layer assesses this under a strictly defined emergency policy. If approved, the decision is marked as emergency, and the declared delivery is linked to both that status and the necessary explanation provided during the policy window in later records. The chain makes emergency use extremely visible and auditable, but it does not reveal any clinical content. This balances the demands of accountability with the need for prompt care: extraordinary access is feasible, but it must be limited, noticeable, and reviewable.

Success criteria

- Emergency authorisation is limited to predefined minimum-necessary categories and flagged as emergency.
- Obligations exist and are linked.
- Emergency use is conspicuous in audit and never broadens the scope of normal consent.

Verifiable properties

- Emergency decisions are distinguishable by policy flag and restricted scope codes.
- A justification record is present within the policy window, or the episode is flagged overdue.
- All emergency entries carry qualified timestamps and inclusion proofs; no health personal data appears on-chain.

The flow of the use case is demonstrated in Figure 8.

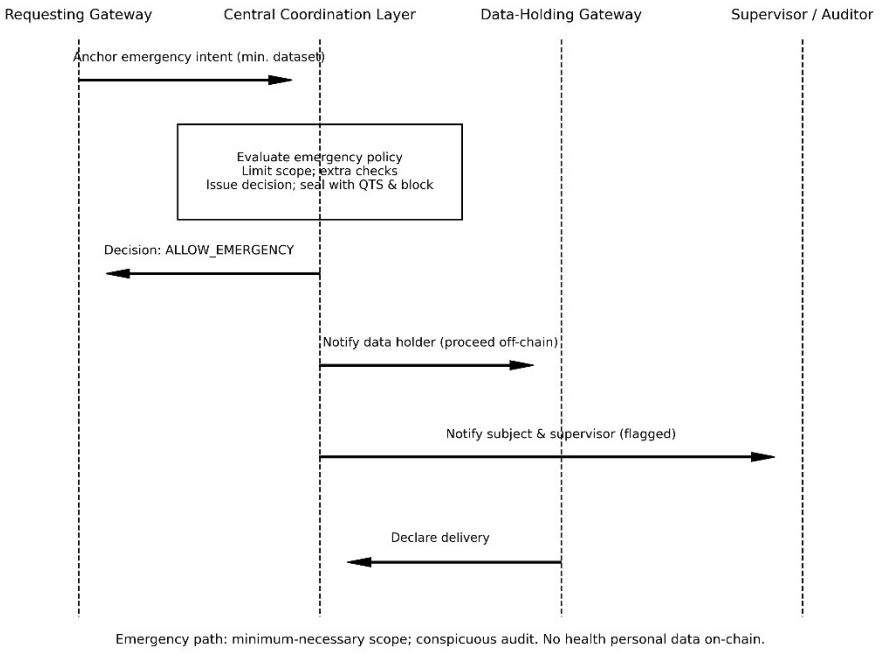


Figure 8 - Use case 4 Diagram example of communication

4.2.5. Use Case 5: Revoking the request

Consent for the relevant scope may be withdrawn at any time by the data subject or a competent authority acting in the home context. The central layer establishes an explicit cutoff after which requests for the same subject-scope-requester tuple are no longer executable by recording the revocation with trusted time and order. The ledger's narrative enables an authorised reader to

confirm that no "Allow" decisions were made after the revocation time, and any subsequent intent anchored after that cutoff deterministically yields a "Deny." By keeping health-related personal information off the blockchain, this behaviour transforms the ability to revoke consent into a system property that is immediately effective upon commitment and verifiable without reference to off-chain logs.

Success criteria

- Revocation is recorded with trusted time and order; subsequent requests for the same subject, scope, and requester are non-executable.
- No Allow occurs when the evaluation time is on or after the revocation's effectiveness.
- Audit shows an explicit cutoff.

Verifiable properties

- "No Allow after T" holds for the tuple once revocation is committed.
- Later attempts produce Deny with a revocation reference and a qualified timestamp.
- The evidence bundle shows revocation → later denial ordering unambiguously.

The flow of the use case is demonstrated in Figure 9.

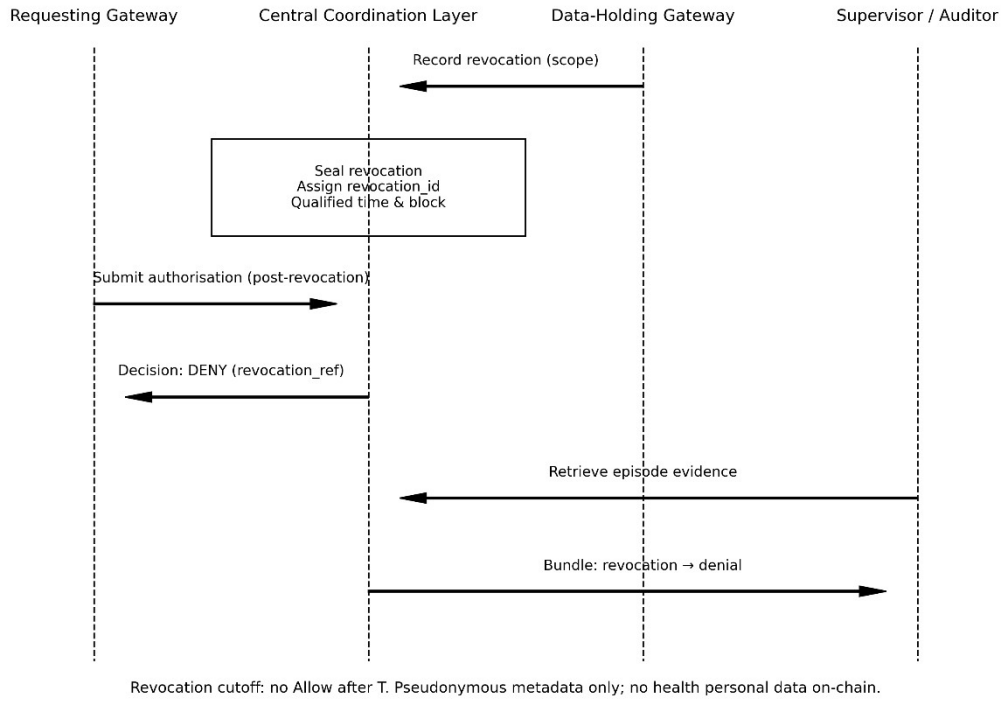


Figure 9 - Use case 5 Diagram example of communication

4.3. Real World Use Case Example

Porto is the temporary home of an Estonian patient undergoing oncology follow-up at IPO Porto. The clinical team requires the most recent discharge summary and medication history from Estonia during a consultation in the city. The Portuguese national blockchain (PT-BC) receives an access request from the Portuguese hospital. A proof-carrying AccessIntent is created by PT-BC's national relay and anchored on the Central EU Coordination Blockchain. Only coded scope/purpose, a pseudonymous subject handle, and a requester handle bound to eIDAS-recognised organisational credentials are included in the intent.

PT hospital → PT-BC

The Portuguese hospital submits a domestic access request to PT-BC.

PT-BC relay → Central EU chain

The Portuguese national relay anchors ex*: AccessIntent{scope: meds, discharge; purpose: continuity_of_care; episode_id}* on the central chain.

Central EU chain

The Authorisation Oracle evaluates:

- Membership/role of the Portuguese requester.
- Consent-token presence and validity window for the subject/scope/requester tuple. Outcome: *Decision = Allow (or Deny)*, sealed with a qualified timestamp and block reference.

Off-chain exchange (EE ↔ PT)

On Allow, the Estonian provider transfers the requested clinical payload directly to the Portuguese provider over a secure, standards-based channel.

Audit completion

- Estonia → *DeliveryAcknowledged{episode_id}*.
- Portugal → *ReceiptLogged{episode_id}*.

Consent change → revocation semantics

If the patient narrows or withdraws consent, PT-BCs relay records *Revoke{scope = discharged_summaries}* on the central chain, establishing an unambiguous cut-off T.

Oversight (subject/regulator/auditor)

Role-bounded queries reconstruct the episode end-to-end intent → decision → delivery → revocation without exposing personal data concerning health. Evidence is suitable for supervisory verification and independent assurance.

The functional requirements mapped to the use case, along with the fields required for the flow to function as intended, are shown in Table 6. Since the use case example in this work does not specify an emergency, FR-07 is excluded because it is designed for emergency use.

Table 6 - Functional Requirements Mapping

FR	Where it appears in the flow	Evidence/fields on the central layer
FR-01	Step 2 (PT-BC relay anchors AccessIntent); Step 3 (Authorisation)	requester_handle, org signature, membership state; mutual TLS assumed
FR-02	Step 3 (Authorisation: membership/role check)	Membership registry: requester_handle admitted; policy_version
FR-03	PT hospital triggers a consent request via PT-BC before AccessIntent	consent_token_handle created/updated on PT-BC, minimal reference published to EU
FR-04	Initial Allow (approval exists); later "scope narrowing" (revocation recorded)	consent_token_handle lifecycle events; revocation_ref; qualified timestamp
FR-05	Step 3 (EU Authorisation Oracle checks PT consent presence/scope/validity)	consent_token_handle reference checked; scope_code, purpose_code, validity window
FR-06	Step 4 (EE → PT off-chain transfer only after Allow); EE validates before sending	Off-chain check by EE of decision + scope; on-chain linkage via decision_id
FR-08	Step 5 (DeliveryAcknowledged/ReceiptLogged); oversight queries	episode_id, decision_id, delivery_receipt_id, inclusion proofs, qualified timestamps
FR-09	Step 2 & revocation step (PT-BC publishes minimal fingerprints to the EU)	Publishing consent_token_handle refs; Access events (no health data)
FR-10	Step 4 (off-chain payload transfer); privacy stance throughout	"No health personal data on the central chain"; off-chain standards (e.g., EHRxF/FHIR), secure channel

The use of Smart Contracts in this operation is described in Table 7.

Table 7 - Smart Contracts used in Use Case

Smart Contract	Operation	Use in Portugal → Estonia use case
SC-01	Admit, update, suspend participants and their roles (requester, data holder, supervisor/regulator, national relay, EU gateway).	Confirms that the Portuguese national relay and the Estonian gateway are active and allowed to act as requesters/data holders before the AccessIntent and the decision are accepted.
SC-02	Register and update recognised healthcare provider identities (institutions and, where applicable, licensed professionals).	Ensures that the Portuguese hospital and the Estonian provider referenced in the episode correspond to registered, trusted organisations.
SC-03	Create, narrow (amend), revoke, and expire cross-border-valid consent tokens.	Holds the patient's cross-border consent from Portugal. The Authorisation Oracle checks here whether valid tokens exist for "medication history" and "discharge summaries," and later reads the revoked scope when Portugal narrows consent.

SC-04	Evaluate access requests and emit allow/deny decisions grounded in consent state and membership status.	Takes the Portuguese AccessIntent, consults membership and consent state, and returns Allow (before revocation) or Deny (for any request that includes a revoked scope).
SC-06	Append immutable lifecycle and access events; assemble verifiable evidence bundles for oversight.	Logs the key events: AccessIntent, Allow/Deny decision, Estonian delivery acknowledgement, and later consent revocation, so that the entire episode can be reconstructed.
SC-07	Bind decisions and lifecycle changes to trusted time and a ledger to ensure revocation is effective.	Timestamp and order the decision and the revocation, making it provable that no Allow occurs after the revocation time for the revoked scope.
SC-09	Provide role-appropriate querying and reporting for subjects, providers, and supervisors/regulators.	Lets the patient, Portuguese and Estonian organisations, and regulators view the Portugal → Estonia episode with different levels of detail, without exposing health data on-chain.

When combined, these smart contracts carry out the guarantees that the Portugal → Estonia use case aims to demonstrate. The Consent Token Registry and the Authorization Oracle transform the legal basis into a deterministic allow/deny outcome for each access intent. At the same time, Membership & Roles and the Provider Trust Register guarantee that only approved, trusted organisations can participate. It is possible to demonstrate that no authorisations occur after a revocation time for a revoked scope, because the Cross-Border Audit & Evidence Ledger and the Time & Ordering Authority provide that result through a tamper-evident, time-ordered trail. The Observability & Transparency Interface exposes the entire episode to subjects, providers, and supervisors without ever putting health-related personal data on the chain. At the same time, Governance & Parameters establishes the policy environment (scope codes, consent durations).

4.4. GDPR Alignment

Any processing of health-related personal data is subject to stringent guidelines set forth by the General Data Protection Regulation, including lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. The burden of proving compliance becomes crucial in a cross-border situation. For this reason, the central coordination layer is purposefully small. Only the minimal coordination metadata, such as consent presence and lifecycle, authorisation outcomes, and audit events, necessary to demonstrate lawfulness are recorded. Clinical content is never processed. This division enables an EU-level framework to verify the timing and legality of

exchanges without disclosing health information, while maintaining national sovereignty over clinical records. Instead of being an afterthought, data protection is integrated as architectural defaults. Only coded, pseudonymous metadata is stored in the ledger, read paths are denied by default, and no health data is written to it. Qualified timestamps are used during block sealing to resolve temporal ambiguities, ensuring that statements such as "non-executability after T" have a clear impact. Bridges use hardware-backed keys, nonces and validity windows to enforce replay resistance, and mutual TLS with eIDAS-recognised organisational credentials. To ensure transparency and traceability at the governance level, parameter changes and membership actions are recorded on-chain.

The model also addresses the common conflict between immutability and data subject rights. Rewriting history is unnecessary for rectification and erasure, since clinical content and direct identifiers are not included in the ledger. An append-only update designates the previous entry as inoperative and provides updated metadata if a correction is needed, such as an incorrect scope code attached to an intent. Audit queries are necessary to resolve to the effective state. While strict minimisation and pseudonymization lessen the residual risk associated with deletion requests while still permitting supervisory oversight, subjects maintain visibility over their own interactions through a role-bounded evidence view.

Before deployment, a Data Protection Impact Assessment is necessary due to the sensitivity and scope of cross-border coordination. The outline is clear even in a theoretical treatment: explain the processing (coordination metadata only), describe the necessity and proportionality (why the narrowest effective mechanism is a minimal, permissioned ledger), identify risks (replay, role misuse, linkability), and document mitigations (qualified time, role-bounded access, pseudonymous handles, controlled code sets, and transparent governance). To clarify responsibilities for data subject rights and incident response, the DPIA should be supplemented by a joint-controllership arrangement and processing records that differentiate the central coordination purpose from national clinical processing.

Lastly, consent withdrawal must work as well in reality as it does in theory. The consent-token lifecycle gives that guarantee a tangible form: any subsequent authorisation for the same subject, scope, and requester becomes non-executable, and revocation is recorded with trusted time and deterministic ordering. Without revealing health information, this transforms a legal right into a verifiable system property. The monotonic nature of scope amendments enhances patient control while maintaining a logical audit trail for regulators and auditors.

CHAPTER 5

Conclusions

5.1. Restatement of the Problem and Objectives

In Europe, cross-border sharing of healthcare data is necessary to promote public health and continuity of care, but current systems are still disjointed and compartmentalised. The goal of a unified EHDS is undermined by the fact that patient records are frequently stuck in separate national or institutional databases. When patients travel between member states, this fragmentation and inconsistent standards result in poor interoperability and gaps in care. Sensitive health information is also becoming increasingly vulnerable under existing frameworks, and cyberattacks and data breaches remain significant threats. Ensuring strong privacy and security across various systems has been challenging. The way that current governance regimes, such as the implementation of GDPR or ISO standards, protect health data has drawn criticism from stakeholders. Necessary legal requirements, such as obtaining and upholding patients' consent preferences and providing audit trails of data use, are still challenging to implement consistently in practice. Without a central way to verify compliance, trust between organisations is fragile. For instance, under the current self-reporting model, a hospital might violate a patient's consent or even hide a breach, leaving authorities in the dark. These issues highlight the need for a novel approach to cross-border health data exchange that improves interoperability, ensures privacy-by-design, and provides verifiable accountability.

The thesis began with three primary goals to address this issue. Initially, it aimed to assess critically whether blockchain technology could successfully satisfy the strict regulations of EU healthcare data management and how it stacks up against other strategies. This required identifying potential disadvantages (such as scalability limitations) and investigating whether blockchain's features, such as decentralisation, immutability, and distributed trust, can improve security, privacy, and interoperability for electronic health records. Second, the study sought to comprehend the European regulatory framework governing health data and to review and organise the body of knowledge already available on blockchain in healthcare. The objective was to identify best practices and gaps in implementing blockchain in line with EU regulations by reviewing the literature and industry initiatives. Third, based on these observations, the thesis proposed a conceptual solution architecture (a proof-of-concept design) for an EU-wide "blockchain layer" that would monitor and manage cross-border healthcare data sharing.

5.2. Positioning of My Thesis and Its Contribution

Many studies in the literature on blockchain in healthcare focus on improving data security, privacy, and interoperability at the regional or national level. The difficulty of creating a cross-border coordination layer that enables safe, interoperable healthcare data exchange among EU member states, however, has not received much attention.

To close this gap, my thesis proposes a blockchain-based coordination layer that serves as a middleman between independent healthcare systems, ensuring the secure transfer of medical data across nations while complying with national laws and patient consent requirements. My research focuses on the practical implementation, regulatory compliance, and governance mechanisms necessary for EU-wide interoperability, in contrast to earlier work that primarily focuses on institutional-level blockchain applications or theoretical proposals for cross-border exchange.

5.3. Answers to the Research Questions

The three research questions from Chapter 1 are reviewed in this section, which summarises how each is addressed by the suggested architecture and its theoretical assessment, highlighting both the contributions and the lingering drawbacks.

How can blockchain technology address the current challenges in cross-border healthcare data exchange within the European Union?

The analysis in this thesis demonstrates that blockchain can address several structural issues in the European health data landscape, including weak cross-organisational trust, data fragmentation, and the lack of verifiable audit trails. Without centralising protected health information, the design creates a shared trust fabric across national systems by implementing an EU-level coordination chain that records only minimal, pseudonymous metadata. The meta-chain creates continuous, tamper-evident narratives for cross-border exchanges by anchoring access intents, the presence of consent tokens, deterministic authorisation decisions, and episode-complete audit events. Clinical content continues to flow through standards-based channels like FHIR/EHRxF profiles and is stored and transported by national ledgers and current infrastructures. When combined, these components reduce data silos, improve accountability, and allow patients and supervisory authorities to reconstruct who accessed what, when, and under what legal basis.

In practical terms, the proposed artefact tackles interoperability and trust through a limited number of design decisions: a membership and roles registry based on eIDAS-recognised organisational credentials, an EU meta-chain that facilitates cross-border consent verification, a consent-token model with clear scope and validity and smart contracts that convert legal conditions into deterministic "Allow" or "Deny" results. Together, these mechanisms support continuity of care while upholding national sovereignty and EU-level regulatory constraints, as demonstrated by the Portugal–Estonia use case and the document-based evaluation. Blockchain is best viewed as a coordination and assurance layer rather than a comprehensive solution to all integration issues because interoperability at the semantic level still depends on national implementations and external standards.

To what extent can a permissioned blockchain model enhance privacy and consent management of electronic health records in compliance with GDPR and other EU regulations?

The results show that, if its scope is carefully limited, a permissioned blockchain model can significantly improve consent management and privacy protection for cross-border health data exchange. The suggested architecture deliberately keeps all clinical content and direct identifiers off-chain and processes only pseudonymous coordination metadata, such as qualified timestamps, scoped access intents, and hashed consent-token handles. While the use of organisational certificates and mutual TLS at the perimeter complies with eIDAS requirements for identity assurance, this stringent data minimisation, along with controlled vocabularies for scope and purpose, supports the principles of lawfulness, purpose limitation, and data minimisation under GDPR. Key GDPR rights, such as explicit consent, the right to withdraw consent, and the requirement for accountability, are translated into machine-enforceable system properties by the consent-token lifecycle, deterministic revocation semantics, and a narrowly bounded emergency access path.

The assessment also recognises significant limitations and trade-offs. There are still residual privacy risks at the metadata level. If governance and role separation are not strictly enforced, repeated queries or unusual access patterns could, in theory, allow inference about patient trajectories even in the absence of clinical content. The model also assumes that clinical systems, national gateways, and off-chain identity management are appropriately set up and run. Poor key management or insufficient access control in these areas would compromise the ledger's guarantees. Furthermore, comprehensive Data Protection Impact Assessments, cooperative controllership agreements, and unambiguous incident-response protocols remain necessary for a permissioned blockchain. Therefore, the thesis concludes that a permissioned

blockchain can significantly improve consent governance and privacy by design, but only as a component of a larger socio-technical and regulatory framework rather than as a stand-alone protection.

What are the functional and non-functional requirements for building a blockchain-based EU coordination layer for healthcare data exchange?

Ten functional and ten non-functional requirements are identified and systematised in the thesis, which together define the parameters within which an EU coordination layer must function. Functionally, the system must support explicit consent requests and revocations, maintain a provider trust registry, enable cross-border consent verification and authorisation at the data holder, provide a tightly controlled break-glass path for emergencies, generate immutable audit trails and views, synchronise minimal metadata between national and EU ledgers, and guarantee standards-based, off-chain exchange of clinical content. These components are directly instantiated in the smart-contract layer and message flows of the suggested architecture, as shown in Table 2. Cryptographic security and key management, privacy and minimisation, GDPR and EHDS alignment, auditability and non-repudiation, syntactic and semantic interoperability, latency, availability and resilience, timely revocation propagation, maintainability, and governance in a multi-state consortium are among the non-functional requirements listed in Table 3.

At least during the design phase, the theoretical evaluation shows that these requirements are internally consistent and can be met by the suggested design. The mapping in Tables 5 and 6 connects each stage of the flow to requirements and smart contracts, while the five use cases and the actual Portugal–Estonia scenario demonstrate how the functional requirements are applied in tangible cross-border episodes. The three analytical lenses: privacy by design and proportionality, audit/evidence/oversight, and regulatory compliance, make the case that the non-functional envelope is respected by, for instance, enforcing deterministic revocation semantics, guaranteeing role-bounded transparency, and upholding strict separation between coordination metadata and clinical data. However, the thesis acknowledges that additional empirical work, such as prototyping, performance and resilience testing, and stakeholder engagement to verify usability, governance feasibility, and real-world proportionality, would be necessary to validate these requirements fully.

5.4. Practical Implications for Member States

The proposed EU blockchain layer would have significant practical ramifications for Member States and their healthcare stakeholders if implemented. First, the European blockchain network would need to be integrated with each Member State's national health information infrastructure. This entails setting up a national gateway service that can connect regional EHR systems to the EU-wide ledger. Current national platforms would be modified to query the blockchain upon requests for access to foreign data and to publish consent tokens and audit logs to the blockchain. To manage the additional workflows (e.g., ensuring that a standardised metadata record is generated and written to the chain whenever a patient gives consent to cross-border data sharing), Member States may need to invest in upgrading their systems. To ensure that all participants describe data access events and consents consistently, interoperability standards such as the European EHR Exchange Format will be crucial to this integration.

Another important implication is governance: under the direction of an EU governing body, the blockchain network would essentially establish a coalition of national health authorities. The infrastructure's operation would probably be divided among the member states. In addition to distributing trust and control fairly among nations, this collective model necessitates close collaboration and consensus on regulations (such as membership requirements, node security, and update protocols). The ledger's audit trail would enable national supervisory authorities to provide real-time oversight of cross-border data transactions. Because regulators in every nation could be automatically notified of irregular or unauthorised access, they could act more quickly, thereby strengthening enforcement of GDPR and EHDS provisions.

An EU blockchain layer standardises and makes consent and access management for patients and healthcare providers more transparent. A patient in one nation could simply give or withdraw consent for a physician in another to view their records, and both the patient and the providers would have an unambiguous, reliable record of those decisions. However, for clinicians and data managers to comprehensively understand procedures (such as verifying the EU ledger for consent before retrieving data), Member States must ensure appropriate training and change management. In general, implementing a blockchain-based coordination layer would encourage Member States to adopt more proactive compliance, cooperative governance, and technical standardisation in the field of digital health. By providing the technical foundation for trust, it operationalises the objectives of European initiatives such as the EHDS. However, its success will rely on each nation's dedication to modifying local workflows and systems to fit this new paradigm.

5.5. Limitations and Threats to Validity

Although this study offers a conceptual roadmap, it is crucial to recognise its shortcomings and associated validity risks. Without a full-scale implementation or live pilot, the suggested blockchain architecture and its assessment were carried out through design analysis and reasoning, making the work fundamentally theoretical. Consequently, it was not possible to directly observe practical issues that would arise in a real deployment. This reduces the confidence that the solution will work perfectly in real-world situations. Instead of using empirical measurements, the evaluation relied on reasoning grounded in design principles and regulations, introducing some subjectivity and assumptions.

Additionally, the research's scope was limited. The design addresses consent, access control, and audit for the primary use of health data, which is international patient care. The solution may need to be significantly extended or modified to cover those scenarios, as it does not thoroughly examine the secondary use of data (research and analytics), another pillar of the EHDS. Furthermore, some technical aspects were abstracted; for example, specific interoperability standards and user identity management issues (beyond assuming eIDAS-compliant IDs) were outside the immediate purview. This indicates that integration with current national systems and standards, such as national patient portals or HL7 FHIR, was not tested and may present difficulties. Even though a systematic review was conducted, the field of blockchain in health IT is rapidly developing, which poses another limitation regarding timing and literature coverage.

5.6. Risk Considerations and Mitigations

There are several risks associated with implementing an EU-wide health blockchain that need to be proactively managed. Technical risk is one important category. This includes the potential for smart contract software flaws or vulnerabilities to be used to circumvent consent requirements or tamper with audit logs. Performance bottlenecks are another risk, if the blockchain network is unable to grow to accommodate the volume of transactions, it may impede the flow of vital information. Before any production rollout, thorough testing and security audits of the smart contracts and platform would be necessary to reduce these technical risks. To monitor performance in a controlled environment, the system could be introduced gradually (for example, by piloting it with specific data types or between particular regions). Additionally, throughput and latency can be kept within reasonable bounds by selecting a

scalable consensus mechanism and optimising transaction payloads. To ensure the infrastructure keeps up with increasing usage, regular capacity planning and network upgrades are crucial.

Trust and governance pose a serious risk as well. A cross-border blockchain's success depends on Member States' continued cooperation. If nations don't agree on policies or the consortium lacks clear dispute-resolution procedures, governance may fail. Here, mitigation entails building a strong governance structure from the start, including explicit participation guidelines, legal agreements supporting the consortium, and an EU-level supervisory board to oversee and mediate. The network can better withstand organisational or political upheaval by defining roles and implementing fail-safes (such as the ability to freeze or revert a smart contract in the event of a serious bug, through multi-party agreement). The legal risk associated with governance includes questions about how current laws apply to blockchain records and potential liability issues if something goes wrong. Careful design (as in this thesis, avoiding on-chain personal data to avoid GDPR erasure conflicts) and gaining regulatory support can help mitigate these. During implementation, close collaboration with legal experts will ensure that the system's functions remain within the parameters of EU law and can adapt to new legal interpretations.

Risks to privacy and security must also be considered. Even though the system is built with privacy in mind, there is always a chance that metadata could be used to identify patients. Another risk is a breach of credentials, such as a hospital's private key to its blockchain, which could enable an attacker to access permissions or falsify records. Strong authentication procedures and the use of hardware security modules for key storage are examples of mitigation techniques. Finally, adoption risk is significant because end users (such as hospitals, physicians, and patients) may find ways to circumvent the new system or delay its use, which would limit its effectiveness. It will be crucial to establish trust through education, emphasising that the blockchain layer protects patient rights by design and that it facilitates, rather than hinders, data sharing. This risk can also be reduced by offering incentives for adoption.

5.7. Future Work

Building on this thesis, a few directions for further investigation become apparent. Implementing a prototype of the suggested EU blockchain for health data would be a crucial next step. The purpose of such a prototype would be to verify the system's security, scalability, and performance in an operational simulation. A small number of cross-border transactions between Member States or healthcare facilities could be used for testing, measuring factors such as transaction throughput, latency during consent verification, and resilience to network disruptions or node failures. Penetration testing could also be conducted during this experimental phase to evaluate the efficacy of the proposed privacy-preserving measures, such as the robustness of access control via smart contracts and the pseudonymization of on-chain metadata.

Investigating how the suggested blockchain layer might work with ongoing European digital health projects is crucial. Redundancy would be avoided, and policy coherence would be guaranteed by aligning the architecture with the EHDS implementation roadmap. Real-world viability will depend on integration with national electronic health infrastructures, especially those that use standards like the European EHR Exchange Format, and with identity assurance mechanisms under the eIDAS framework, such as the European Digital Identity Wallet. As national systems continue to oversee patient interfaces and clinical data storage, these links would allow the blockchain to operate as a reliable coordination fabric.

Lastly, systematic interaction with healthcare stakeholders, such as providers, patients, technology specialists, and regulators, should be a part of future research. These actors can assist in improving the operational workflows and governance model described in this thesis through interviews, workshops, or pilot studies. Adoption will depend on how patients view the system's transparency and control, or how clinicians engage with consent and audit mechanisms in practice. Investigating different governance models, such as a federated model with Member State autonomy versus a central EU-led consortium, may also provide significant insights into administrative overhead, legal accountability, and trust distribution. This stakeholder-driven effort will ensure that the proposed blockchain solution aligns with the socio-technical environment of European healthcare and the theoretical standards of compliance and auditability.

5.8. Final Remarks

In summary, this thesis has investigated how an EU-wide blockchain-based coordination layer could revolutionise cross-border health data sharing, providing a fresh approach to persistent interoperability and trust issues. The research contributes to a vision of patient-centric, privacy-preserving interoperability in the EU by thoroughly analysing requirements and regulations, reviewing the state of the art, and putting forth a concrete architecture. The suggested strategy shows that it is possible to balance the frequently conflicting goals of data availability and confidentiality. By making design decisions that prioritise consent, auditability, and minimal exposure of personal data, the solution upholds the GDPR-mandated privacy-by-design ethos while allowing information to flow where and when it is required for patient care. Additionally, a neutral trust layer that can promote increased confidence among Member States participating in data exchange is provided by anchoring the system at the EU level through a central blockchain not controlled by any one nation. It provides a practical way to achieve the objectives of the European Health Data Space by connecting national systems under standardised guidelines and cryptographic safeguards rather than replacing them.

It goes without saying that the transition from conceptual design to practical implementation is complex. Realising this vision will require policy development, technical improvements, and stakeholder consensus-building. The conclusions and framework discussed here provide a basis for future research and communication between technologists, medical professionals, and regulators. It is crucial to make sure that this progress is accompanied by robust data governance and respect for patient rights as Europe's health sector continues to digitise and integrate. In the end, the thesis emphasises that blockchain technology should be viewed as an enabling tool rather than an end in itself, a means to create a health data ecosystem that is more secure, transparent, and interoperable for the benefit of all EU citizens.

The ideas presented in this work can guide future efforts to create a reliable pan-European health information infrastructure in which patients can travel safely and their data follow securely, voluntarily, and are auditable at every stage, with careful stewardship. The convergence of policy momentum and technological capability presents a unique opportunity, but bringing together the healthcare systems of more than two dozen countries is an enormous challenge. This final chapter reiterates that the European Union can move closer to a future in which patient empowerment and privacy are upheld. At the same time, health data transcends national boundaries by embracing creative solutions and cooperative governance.

Bibliographic References

[1] A. Ahmed, A. Shahzad, A. Naseem, S. Ali, and I. Ahmad, 'Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: A quantitative analysis of ISO standards, GDPR, and HIPAA in blockchain technology', *PLOS ONE*, vol. 20, no. 5, p. e0324285, de mai. de 2025, doi: 10.1371/journal.pone.0324285.

[2] B. P. Pokharel, N. Kshetri, S. R. Sharma, and S. Paudel, 'blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems', *Information*, vol. 16, no. 2, Art. no. 2, Feb. 2025, doi: 10.3390/info16020133.

[3] Yaqub N, Zhang J, Khalid MI, Wang W, Helfert M, Ahmed M, Kim J., 'Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records. PeerJ Computer Science 11:e2647', 2025, [Online]. Available: https://doi.org/10.7717/peerj-cs.2647

[4] 'European Commission, "European Health Data Space Regulation (EHDS).' Accessed: Jul. 09, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500327

[5] 'ISO - International Organization for Standardization', ISO. Accessed: Jul. 19, 2025. [Online]. Available: https://www.iso.org/home.html

[6] 'European Union, "Regulation (EU) 2016/679 (General Data Protection Regulation)," EUR-Lex. 2016'. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

[7] 'U.S. Department of Health & Human Services, "HIPAA Home."' Accessed: Jul. 19, 2025. [Online]. Available: https://www.hhs.gov/hipaa/index.html

[8] I. Román-Martínez, J. Calvillo-Arbizu, V. J. Mayor-Gallego, G. Madinabeitia-Luque, A. J. Estepa-Alonso, and R. M. Estepa-Alonso, 'Blockchain-Based Service-Oriented Architecture for Consent Management, Access Control, and Auditing', *IEEE Access*, vol. 11, pp. 12727–12741, 2023, doi: 10.1109/ACCESS.2023.3242605.

[9] L. D. Costa, B. Pinheiro, W. Cordeiro, R. Araújo, and A. Abelém, 'Sec-Health: A Blockchain-Based Protocol for Securing Health Records', *IEEE Access*, vol. 11, pp. 16605–16620, 2023, doi: 10.1109/ACCESS.2023.3245046.

[10] M. Shaikh, S. A. Memon, A. Ebrahimi, and U. K. Wiil, 'A Systematic Literature Review for Blockchain-Based Healthcare Implementations', *Healthcare*, vol. 13, no. 9, Art. no. 9, Jan. 2025, doi: 10.3390/healthcare13091087.

[11] ‘Ethereum.org, “The complete guide to Ethereum.”’, ethereum.org. Accessed: Jul. 19, 2025. [Online]. Available: https://ethereum.org/en/

[12] Musharraf N. Alruwaill, Saraju P. Mohanty, and Kougianos Elias, ‘hChain 4.0: A Secure and Scalable Permissioned Blockchain for EHR Management in Smart Healthcare’, May 20, 2025, *arXiv*: arXiv:2505.13861. doi: 10.48550/arXiv.2505.13861.

[13] ‘European Commission, “eIDAS Regulation,” Shaping Europe’s digital future.’ Accessed: Jul. 09, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[14] M. J. Page *et al.*, ‘The PRISMA 2020 statement: an updated guideline for reporting systematic reviews’, *BMJ*, vol. 372, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.

[15] N. T S, B. K. Rai, P. P, P. R, and P. M, ‘Blockchain Based Health Insurance System’, in *2025 3rd International Conference on Disruptive Technologies (ICDT)*, Mar. 2025, pp. 1216–1221. doi: 10.1109/ICDT63985.2025.10986743.

[16] P. Verma and A. K. Jain, ‘A Comprehensive Study on the Application of Blockchain Technology’s Use in Healthcare’, in *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, https://ieeexplore.ieee.org/document/10169250, Jun. 2023, pp. 1388–1393. doi: 10.1109/ICSCSS57650.2023.10169250.

[17] ‘Empowering Healthcare: Hyperledger Blockchain for Unified Electronic Health Records and Organ Donation Integrity | Request PDF’, in *ResearchGate*, Feb. 2025. doi: 10.1109/ICBDS61829.2024.10837436.

[18] A. Rai, M. Naik, and I. Seraphim B, ‘Leveraging Blockchain Technology for Secure and Efficient Storage of Medical Data’, in *2024 IEEE 16th International Conference on Computational Intelligence and Communication Networks (CICN)*, Dec. 2024, pp. 652–656. doi: 10.1109/CICN63059.2024.10847418.

[19] A. Galaba, M. Palagani, R. Vinukonda, J. S. P. Malampati, S. S. Harsha, and K. V. D. Kiran, ‘Significance of Blockchain Technology in the Healthcare Sector’, in *2023 International Conference on Inventive Computation Technologies (ICICT)*, Apr. 2023, pp. 1159–1165. doi: 10.1109/ICICT57646.2023.10134196.

[20] A. Koulianos, P. Paraskevopoulos, A. Litke, and N. Papadakis, ‘Towards Enhanced Data Integrity and Accountability: Leveraging Blockchain Technology in Healthcare’, in *Proceedings of the 17th International Conference on PErvasive Technologies Related to Assistive Environments*, in PETRA ’24. New York, NY, USA: Association for Computing Machinery, Jun. 2024, pp. 587–592. doi: 10.1145/3652037.3663889.

[21] A. Z. Nouh Allan, A. M. Y. Albahnasawi, T. Mokhamed, S. Abbas, M. A. Moufti, and M. A. Talib, 'Unified Blockchain-Based Electronic Dental Record Ecosystem for Secure Data Exchange', in *2024 6th International Conference on Blockchain Computing and Applications (BCCA)*, Nov. 2024, pp. 531–537. doi: 10.1109/BCCA62388.2024.10844388.

[22] 'Index - FHIR v5.0.0'. Accessed: Jul. 19, 2025. [Online]. Available: https://www.hl7.org/fhir/

[23] S. Nekkalapudi, R. K. Mishra, and M. Pandey, 'Blockchain-Based Healthcare Outcome Improvement: A Decentralized Method of Patient Care', in *2024 First International Conference on Data, Computation and Communication (ICDCC)*, Nov. 2024, pp. 546–550. doi: 10.1109/ICDCC62744.2024.10961792.

[24] 'e-Estonia - We have built a digital society & we can show you how', e-Estonia. Accessed: Jul. 16, 2025. [Online]. Available: https://e-estonia.com/

[25] 'Guardtime'. Accessed: Jul. 16, 2025. [Online]. Available: https://guardtime.com/en

[26] S. Hankewitz, 'Estonia to protect patient records with blockchain technology', Estonian World. Accessed: Jul. 16, 2025. [Online]. Available: https://estonianworld.com/technology/estonia-to-protect-patient-records-with-guardtime-blockchain-technology/

[27] 'PLA - Digital Trust Ecosystem', PharmaLedger Association. Accessed: Jul. 16, 2025. [Online]. Available: https://pharmaledger.org/

[28] L. Insights, 'PharmaLedger blockchain association launches first product, adds new members', Ledger Insights - blockchain for enterprise. Accessed: Jul. 16, 2025. [Online]. Available: https://www.ledgerinsights.com/pharmaledger-blockchain-association-launches-first-product-adds-new-members/