INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Secure Storage and Management of Medical Imaging in a Patient Wallet Using European Interoperability Standards

Alexandre Rodrigo Machado Torres

Masters in Digital Technologies for Business

Supervisor:
Doctor João Carlos Ferreira,
Assistant Professor with aggregation,
ISCTE, University Institute of Lisbon

Decembre, 2025

TECNOLOGIAS
E ARQUITETURA

Department of Information Science and Technology

Secure Storage and Management of Medical Imaging in a Patient Wallet Using European Interoperability Standards

Alexandre Rodrigo Machado Torres

Masters in Digital Technologies for Business

Supervisor:
Doctor João Carlos Ferreira,
Assistant Professor with aggregation,
ISCTE, University Institute of Lisbon

December, 2025

Acknowledgements

I want to thank my supervisor, João Carlos Amaro Ferreira, for his availability throughout the development of this thesis and for helping ensure that the work remained aligned with the programme's academic requirements. His guidance and feedback shaped the structure and clarity of the work as it evolved into its final form.

I would also like to express my appreciation to ISCTE – University Institute of Lisbon for the academic environment and training provided throughout the programme. I am grateful to all the lecturers and teaching staff whose courses, discussions, and guidance contributed to the knowledge base and critical perspective that informed this thesis.

I also wish to thank my colleagues for their support and for the informal discussions that helped clarify concepts, challenge assumptions, and sustain motivation during the more demanding phases of the work. Those exchanges, even when brief, were valuable in keeping the work grounded and moving forward.

This thesis was completed during a particularly challenging year, marked by significant professional and personal changes. It required persistence and a stable support network, especially during periods when time and focus were harder to protect.

My deepest thanks go to my mother and my partner. I am grateful to my mother for her unwavering encouragement, strength, and steady presence throughout this period, as well as for the practical support that helped me remain consistent. I am equally grateful to my partner for their patience, understanding, and day-to-day support, which made it possible to carry this work through moments of uncertainty and change. Their support was fundamental to bringing this thesis to completion.

Resumo

A crescente necessidade de uma gestão segura e interoperável dos dados de imagiologia médica na Europa, juntamente com iniciativas como o Espaço Europeu de Dados de Saúde (EHDS) e o Formato Europeu de Intercâmbio de Registos de Saúde Eletrónicos (EEHRxF), está a impulsionar os sistemas de saúde para além dos silos centrados nas instituições, rumo à partilha de dados controlada pelos pacientes. Ao mesmo tempo, a conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD), os Serviços de Identificação, Autenticação e Confiança Eletrónicas (eIDAS) e a futura legislação secundária do EHDS exige mecanismos robustos para o consentimento, a responsabilização e a minimização de dados. Neste contexto, a tese examina como a blockchain, os identificadores descentralizados e o armazenamento fora da cadeia (por exemplo, IPFS) podem apoiar uma carteira de imagens centrada no paciente que reforça a integridade dos dados, a gestão do consentimento e a auditabilidade, mantendo-se alinhada às normas europeias de interoperabilidade.

Baseado na Metodologia de Investigação em Ciência do Design (DSRM), o trabalho combina uma revisão estruturada da literatura com uma análise do DICOM/DICOMweb, HL7 FHIR, EEHRxF e MyHealth@EU, a partir da qual se derivam requisitos funcionais e não funcionais para uma carteira de imagens do paciente. Com base nisso, propõe uma arquitetura conceitual modular que utiliza uma blockchain autorizada para consentimentos e políticas invioláveis, identidade descentralizada para pacientes e profissionais, e armazenamento criptografado fora da cadeia para objetos DICOM identificados por identificadores estáveis.

O modelo é concretizado como uma prova de conceito em fase de projeto, expressa por meio de percursos representativos do utilizador para carregamento, partilha transfronteiriça, revogação e auditoria. A avaliação dos requisitos derivados e das restrições de conformidade europeias indica que uma carteira de imagens baseada em blockchain e ancorada em normas é conceitualmente viável e pode melhorar o controlo do paciente e a interoperabilidade transfronteiriça. A análise também destaca a necessidade de futuros trabalhos empíricos sobre implementação, desempenho, usabilidade e governança.

Palavras-chave: Blockchain; Identidade descentralizada; Carteira de saúde do doente; Imagiologia médica; DICOM; FHIR; European Health Data Space

Abstract

The growing need for secure, interoperable management of medical imaging data in Europe, together with initiatives such as the European Health Data Space (EHDS) and the European Electronic Health Record Exchange Format (EEHRxF), is pushing healthcare systems beyond institution-centric silos towards patient-controlled data sharing. At the same time, compliance with the General Data Protection Regulation (GDPR), electronic IDentification, Authentication and trust Services (eIDAS), and the forthcoming EHDS secondary legislation requires robust mechanisms for consent, accountability, and data minimisation. In this context, the thesis examines how blockchain, decentralised identifiers, and off-chain storage (e.g., IPFS) can support a patient-centric imaging wallet that strengthens data integrity, consent management, and auditability while remaining aligned with European interoperability standards.

Guided by the Design Science Research Methodology (DSRM), the work combines a structured literature review with an analysis of DICOM/DICOMweb, HL7 FHIR, EEHRxF and MyHealth@EU, from which it derives functional and non-functional requirements for a patient imaging wallet. On this basis, it proposes a modular conceptual architecture that uses a permissioned blockchain for tamper-evident consent and policy states, decentralised identity for patients and professionals, and off-chain encrypted storage for DICOM objects referenced by stable identifiers.

The design is instantiated as a design-time proof of concept, expressed through representative user journeys for upload, cross-border sharing, revocation and audit. Evaluation against the derived requirements and European compliance constraints indicates that a blockchain-enabled, standards-anchored imaging wallet is conceptually feasible and can enhance patient control and cross-border interoperability. The analysis also highlights the need for future empirical work on implementation, performance, usability and governance.

Keywords: Blockchain; Decentralised identity; Patient wallet; Medical imaging; DICOM; FHIR; European Health Data Space.

Index

Acknowledgements i
Resumo iii
Abstract v
Index vii
List of Figures xi
List of Tables xiii
ACRONYM xv
Chapter 1. Introduction 1
1.1. Research Motivation 1
1.1.1. Technological Perspective 2
1.1.2. Healthcare Relevance 2
1.1.3. Interoperability and Data Sovereignty Challenges 3
1.2. Problem Statement 4
1.3. Research Objectives 5
1.4. Contributions of this thesis 6
Chapter 2. Related Work 7
2.1. PRISMA Methodology 7
2.1.1. Information Sources 7
2.1.2. Search Strategy 7
2.2. Literature Review 10
2.2.1. Enabling Technologies 11
2.2.2. Imaging-oriented use cases 11
2.2.3. Interoperability and Compliance 12
2.2.4. Gaps in the Literature and Research Opportunity 13
2.3. World Case Review: Real-World Implementations of Blockchain in Health Data Management 14
Chapter 3. Conceptual Architecture and Compliance Baseline 17
3.1. Methodological Approach and Scope 17
3.1.1. Research questions as design drivers 17
3.2. Functional and Non-Functional Requirements 18
3.2.1. Functional Requirements 18

3.2.2. Non-Functional Requirements 19
3.2.3. Design-time assumptions and constraints 19
3.3. Reference layered model and architectural baseline 20
3.3.1. Architectural Decision Record summary 25
3.3.2. Interface profile anchors 25
3.3.3. Governance preview 26
3.4. Standards and Legal Compliance Mapping 27
3.4.1. Conformance and verification hooks 27
3.5. Chapter summary and transition 28
Chapter 4. Proof-of-Concept Design and Evaluation Method 29
4.1. Purpose and scope 29
4.2. Conceptual architecture 30
4.2.1. Actors and Trust Boundaries 30
4.2.2. Key Layers of the Architecture 30
4.2.3. Trust and Security Features 31
4.2.3.1. Threat model and mitigations 32
4.2.3.2. Design-time service-level objectives 33
4.2.4. Cross-border Data Exchange 33
4.2.5. Consortium governance 34
4.3. Interoperability assumptions 34
4.4. Privacy and consent model 35
4.4.1. DPIA sketch and emergency access 36
4.5. User journeys 38
4.5.1. J1 – Patient upload 38
4.5.2. J2 – Cross-border share 39
4.5.3. J3 – Revocation 41
4.5.4. J4 – Audit inspection 43
4.6. Evaluation approach at design-time 44
4.7. Findings and open issues 45
4.8. Limitations and validity 46
4.8.1. Scope and methodological boundaries 46
4.8.2. Assumptions underpinning the claims 47
4.8.3. Threats to validity and generalisability 47
4.8.4. Ethical and legal considerations 47

4.8.5. Implications for future evaluation 48
Chapter 5. Discussion and Conclusions 51
5.1. Discussion 51
5.1.1. Restating objectives and research questions 51
5.1.2. Synthesis of findings against RQ1-RQ4 51
5.1.3. Alignment with European standards and policy initiatives 51
5.1.4. Positioning relative to related work and real cases 52
5.1.5. Implications for practice and research 52
5.2. Future Work 52
5.2.1. Technical implementation and performance evaluation 52
5.2.2. Usability, accessibility and clinical integration 53
5.2.3. Governance, legal and ethical consolidation 53
5.2.4. Generalisation beyond imaging and long-term evolution 53
5.3. Concluding Remarks 53

Bibliographic References 55
APPENDICES 59
Appendix A 60
Appendix B 63
Appendix C 65
Appendix D 68

List of figures

Figure 1 - PRISMA of the literature review flow diagram ..... **Erro! Marcador não definido.**
Figure 2 – Modular high-level conceptual architecture of the patient imaging wallet. 23
Figure 3 – Image upload sequence from wallet to off-chain storage and ledger. 24
Figure 4 – Data sharing sequence for the patient imaging wallet. 24
Figure 5 - Upload chooser and selection surface. 68
Figure 6 - Validation and client-side encryption progress. 68
Figure 7 - Consent and integrity anchoring confirmation. 69
Figure 8 - Upload success, study summary and audit entry link..... 69
Figure 9 - Provider selection and study scope screen. 71
Figure 10 - Consent configuration with purpose, validity and verified provider identity. 71
Figure 11 - Consent anchoring confirmation on ledger and share-link preparation. 72
Figure 12 - Share the success summary with a copy link, handoff, and revoke control. 72
Figure 13 - Active shares list with per-grant detail and Revoke control..... 73
Figure 14 - Revocation confirmation with reason code and effect summary. 73
Figure 15 - Revocation anchoring progress with ledger confirmation and time reference. 74
Figure 16 - Revocation success summary with audit link and enforcement note. 74
Figure 17 - Audit timeline with study selector, time window and filter chips. 75
Figure 18 - Event detail panel with links to Consent and Provenance. 75
Figure 19 - Reconstruction progress with correlation to consent state and on-chain anchor check..... 76
Figure 20 - Consolidated narrative and exportable evidence-bundle summary. 76

List of Tables

Table 1 – Search Domains & keywords 7
Table 2 - Steps of document search 8
Table 3 - Documents summary 9
Table 4 - Operationalising RQ1–RQ4 as design drivers 17
Table 5 - Functional requirements of the imaging wallet 18
Table 6 – Non-functional requirements of the imaging wallet 19
Table 7 – Key Layers of the Architecture 31
Table 8 – Trust and Security Features. 31
Table 9 – Minimal cryptographic and governance assumptions. 32
Table 10 – Design-time SLOs for the authorisation and audit path 33
Table 11 – Cross-border Data Exchange 34
Table 12 – Consent states and effects 35
Table 13 – Privacy guarantees and assumptions 36
Table 14 – Overview of user journeys 38
Table 15 – Research question alignment and evidence. 44
Table 16 – Research questions: current evaluation and future empirical work 48
Table 17 - Functional requirements traceability: component, standard, journey, evidence. 60
Table 18 - Non-functional requirements traceability: design mechanism, component, evidence. 61
Table 19 - Minimal evidence bundle fields. 61
Table 20 - Mapping of system requirements to European standards and regulations 62
Table 21 - Architectural Decision Records (accepted) 63
Table 22 - Deferred ADRs (for future implementation/validation). 64
Table 23 - Design-time assumptions and constraints 65
Table 24 - Architecture module mapping. 66
Table 25 - Actors and Trust Boundaries. 67

ACRONYM

ADR	**A**rchitectural **D**ecision **R**ecord
AES	**A**dvanced **E**ncryption **S**tandard
AI	**A**rtificial **I**ntelligence
APIs	**A**pplication **P**rogramming **I**nterfaces
ATNA	**A**udit **T**rail and **N**ode **A**uthentication
CT Scan	**C**omputed **T**omography **S**can
DAG	**D**irected **A**cyclic **G**raph
DICOM	**D**igital **I**maging and **C**ommunications in **M**edicine
DID	**D**ecentralised **I**dentifier
DLT	**D**istributed **L**edger **T**echnology
DPIA	**D**ata **P**rotection **I**mpact **A**ssessment
DSRM	**D**esign **S**cience **R**esearch **M**ethodology
EBSI	**E**uropean **B**lockchain **S**ervices **I**nfrastructure
EEA	**E**uropean **E**conomic **A**rea
EEHRxF	**E**uropean **E**lectronic **H**ealth **R**ecord **E**xchange **F**ormat
EHDS	**E**uropean **H**ealth **D**ata **S**pace
EHR	**E**lectronic **H**ealth **R**ecord
eIDAS	**e**lectronic I**D**entification, **A**uthentication and trust **S**ervices
EIF	**E**uropean **I**nteroperability **F**ramework
EMR	**E**lectronic **M**edical **R**ecord
ENISA	**E**uropean **U**nion **A**gency for **C**ybersecurity
ePI	**e**lectronic **P**roduct **I**nformation
ETSI	**E**uropean **T**elecommunications **S**tandards **I**nstitute
EU	**E**uropean **U**nion
EUDI	**E**uropean **D**igital **I**dentity
FHIR	**F**ast **H**ealthcare **I**nteroperability **R**esources
GDPR	**G**eneral **D**ata **P**rotection **R**egulation
HL7	**H**ealth **L**evel **S**even
HTTP	**H**ypertext **T**ransfer **P**rotocol
IHI	**I**nnovative **H**ealth **I**nitiative
IPFS	**I**nter**P**lanetary **F**ile **S**ystem
KSI	**K**eyless **S**ignature **I**nfrastructure
MRI	**M**agnetic **R**esonance **I**maging
NCPeH	**N**ational **C**ontact **P**oint for **eH**ealth
Oauth	**O**pen **A**uthorization
OECD	**O**rganisation for **E**conomic **C**o-operation and **D**evelopment
OIDC	**O**pen**ID** **C**onnect
PACS	**P**icture **A**rchiving and **C**ommunication **S**ystem
PoC	**P**roof-**o**f-**C**oncept
PRISMA	**P**referred **R**eporting **I**tems for **S**ystematic **R**eviews and **M**eta-**A**nalyses
QIDO-RS	**Q**uery based on **ID** for DICOM Objects using **R**ESTful **S**ervices
REST	**R**epresentational **S**tate **T**ransfer
SLO	**S**ervice **L**evel **O**bjective

STOW-RS	**S**tore **O**ver the **W**eb using **R**ESTful **S**ervices
TLS	**T**ransport **L**ayer **S**ecurity
TTL	**T**ime-**T**o-**L**ive
UI	**U**ser **I**nterface
UMA	**U**ser-**M**anaged **A**ccess
VC	**V**erifiable **C**redentials (VCs)
VNA	**V**endor **N**eutral **A**rchive
WADO-RS	**W**eb **A**ccess to **D**ICOM **O**bjects using **R**ESTful **S**ervices

CHAPTER 1

Introduction

The digital transformation of healthcare is reshaping how medical data are generated, stored and exchanged across the care continuum. Over recent decades, health systems have moved from paper-based records to Electronic Health Records (EHR), enabling faster information flows and new analytical uses of routine clinical data. Yet persistent challenges in interoperability, data security and patient autonomy remain. Health information is still fragmented across institutional and national silos in Europe, where heterogeneous technical standards and governance models hinder seamless data exchange [1], [2]. This fragmentation compromises continuity of care: providers may lack access to complete longitudinal histories, and patients face obstacles when attempting to transfer their records across care settings and borders [2], [3].

In response, the European Union (EU) has advanced the European Health Data Space (EHDS [1]), a regulatory initiative designed to enable secure, cross-border use of health data by promoting common standards, governance mechanisms and technical interoperability [1], [3]. The EHDS is intended to work in conjunction with the European Interoperability Framework (EIF [4]), the General Data Protection Regulation (GDPR [5]), and the electronic Identification, Authentication and trust Services (eIDAS [4]) regime, reinforcing a model of patient-centred, privacy-preserving data governance [3]. Within this policy context, digital health wallets have been proposed to give individuals more direct control over their health information while supporting secure, consent-driven data sharing across jurisdictions [2].

This thesis examines how such wallets, underpinned by blockchain, decentralised identity and EU interoperability standards, can help address longstanding gaps in the management and exchange of medical imaging data.

1.1. Research Motivation

The motivation for this work arises from both technological possibilities and healthcare necessities. Advances in digital technologies have opened new avenues to enhance data control, integrity and privacy. At the same time, the realities of healthcare delivery expose persistent weaknesses in the way sensitive data, such as medical images, is managed. This section frames the relevance of the research from two perspectives, technological (Section 1.1.1) and

healthcare (Section 1.1.2). It highlights interoperability and data sovereignty challenges that make the European context particularly salient (Section 1.1.3).

1.1.1. Technological Perspective

Blockchain and Distributed Ledger Technologies (DLT [6]) are increasingly used to address integrity and trust challenges in health data management. By linking records cryptographically, blockchain ensures that imaging-related records, once written, cannot be altered without detection, providing an immutable audit trail that can support secure consent mechanisms [1], [7]. Smart contracts further allow patients to express granular access conditions and revoke permissions when needed. In parallel, Decentralised Identifier (DID [8]) systems, promoted under the EU's eIDAS framework, enable individuals to store verifiable credentials in personal digital wallets, reducing reliance on central identity providers and strengthening user control over authentication and attribute disclosure [9], [10].

To accommodate the size and complexity of imaging data, hybrid architectures combine blockchain with off-chain storage systems such as the InterPlanetary File System (IPFS [11]). Encrypted image files are stored in distributed networks, while only metadata and hashes are registered on-chain, preserving scalability and integrity [2], [12]. Patients interact with this ecosystem through digital wallets that manage encryption keys, DIDs and verifiable credentials, allowing them to authenticate, grant access and monitor interactions with their data in near real time [7], [9]. The convergence of these technologies, increasingly discussed and endorsed in European and Organisation for Economic Co-operation and Development (OECD [12]) policy work, offers a foundation for secure, interoperable and patient-controlled imaging systems that align with privacy-by-design principles and cross-border health data governance frameworks [1], [10], [12].

1.1.2. Healthcare Relevance

Medical imaging is central to diagnosis, treatment planning and disease monitoring, generating vast volumes of data every day. These images, from routine X-rays to high-resolution Computed Tomography scans (CT scan) and Magnetic Resonance Imaging (MRI) studies, are used throughout a patient's care pathway but are often stored in systems that cannot easily exchange information [7], [12]. This fragmentation leads to delays, redundant imaging and limited patient agency: patients may have to transport scans physically or repeat examinations when moving between providers, both domestically and across borders [3]. At the same time,

imaging files frequently contain identifiable features and are subject to strict privacy requirements under the GDPR. A patient-controlled digital imaging wallet addresses these issues by allowing individuals to securely store and share their imaging records across systems using verifiable consent mechanisms, in line with EU strategies on patient empowerment and data portability within the EHDS framework [1], [2].

Security and privacy risks in the current centralised imaging storage paradigm further reinforce this need. Centralised Picture Archiving and Communication Systems (PACS) and EHR platforms are frequent targets for ransomware and internal misuse, creating systemic vulnerabilities [12], [13]. A decentralised wallet model mitigates part of this risk by giving patients cryptographic control over access, logging all events immutably and enabling consent revocation through smart contracts [7], [9]. This increases transparency and trust while reducing single points of failure. Not all patients wish or are able to manage their data directly, but delegation mechanisms under patient supervision can support inclusivity [2]. By reinforcing privacy, auditability and usability, such an architecture can increase willingness to share data securely, including for secondary uses such as research and Artificial Intelligence (AI [14]) development, and help address clinical, operational and ethical gaps in today's fragmented health information systems.

1.1.3. Interoperability and Data Sovereignty Challenges

Implementing a patient-controlled imaging wallet in the EU is not only a technical endeavour; it must operate within a fragmented landscape of health data infrastructures and regulatory regimes. Member States have developed heterogeneous systems, making cross-border care difficult due to incompatible formats, workflows and legal constraints [3]. The EHDS seeks to reduce this fragmentation by introducing common rules and standards such as the European Electronic Health Record Exchange Format (EEHRxF [15]) and by promoting semantic, technical and legal interoperability through the EIF [1], [4]. In parallel, the eIDAS regulation and the forthcoming European Digital Identity Wallet (EUDI Wallet [16]) provide mechanisms for secure authentication and consent. Aligning the imaging wallet with these frameworks supports patient-centred, cross-border data exchange, while blockchain and smart contracts can help enforce consent and ensure auditability [10].

Respect for data sovereignty, as required by the GDPR, is a guiding principle in the proposed design. Imaging data remain off-chain, encrypted under patient control, with access governed by fine-grained consent expressed via smart contracts [17]. This supports data

minimisation and the right to revoke access. Nevertheless, challenges remain, including uneven Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR [18]) adoption and the incomplete rollout of digital identity infrastructures across Member States [3], By anticipating these limitations and building explicitly on EU standards, the proposed wallet aims to contribute to a secure, interoperable and trustworthy model for managing imaging data within the emerging EHDS ecosystem.

1.2. Problem Statement

Despite significant advances in digital health, there is still no widely adopted solution that allows patients to carry and control their medical imaging data across institutions and borders in compliance with European standards. Existing EHRs and national e-health portals remain fragmented, often vendor-specific and rarely interoperable. Patients treated by multiple providers must juggle several portals or resort to physical media, with no unified, user-controlled platform [2]. These limitations compromise continuity of care, particularly in urgent or cross-border scenarios, and contribute to delays, repeat imaging and loss of critical clinical history [12]. The EHDS aims to address such challenges by promoting common data formats, access rules, and interoperability standards like Digital Imaging and Communications in Medicine (DICOM [19]), FHIR, and the EEHRxF [1], [3]. However, few deployed systems fully adopt these frameworks or provide patients with granular control, and the absence of blockchain-based identity and consent mechanisms continues to limit trust and auditability in data exchange [17].

The impact of this gap extends beyond clinical efficiency. Fragmented and inaccessible imaging data also hinder longitudinal health monitoring and secondary uses such as research, where comprehensive, consent-driven datasets are required to remain compatible with GDPR. While other sectors have begun to deploy decentralised identity and digital wallet models, healthcare adoption remains cautious, constrained by technical complexity and stringent regulation. This thesis therefore proposes a secure, interoperable imaging wallet aligned with EU legal and technical frameworks, giving patients direct control over their imaging data and enabling trusted, standards-compliant sharing across systems. In doing so, it seeks to reduce the distance between current siloed practices and the patient-centric, cross-border digital health infrastructure envisioned in EU policy [10], [5].

1.3. Research Objectives

This thesis addresses a technical and architectural gap in secure, patient-controlled storage and sharing of medical imaging data by pursuing two central objectives.

The first objective is to investigate how emerging technologies, namely blockchain, DID and off-chain storage systems such as IPFS, can be applied to enhance data integrity, consent management and patient control over imaging data. These technologies offer distinct advantages in terms of transparency, verifiability and decentralisation, making them promising enablers for managing sensitive health data in compliance with European regulatory frameworks. In particular, the study explores how blockchain can support tamper-evident audit trails, how DID systems can facilitate secure and user-driven authentication, and how off-chain storage can address the scalability limitations of on-chain data handling, especially for large imaging files.

The second objective is to design a Proof-of-Concept (PoC) architecture for a patient-centric imaging wallet and to specify its behaviour through concrete user journeys. This PoC integrates the above technologies into a coherent system that allows patients to store, view and share their medical images securely. The architecture is aligned with European interoperability standards, such as DICOM for imaging data, FHIR for metadata exchange and the EEHRxF, and with legal frameworks including the GDPR, eIDAS and the forthcoming EHDS. By enabling secure, verifiable and consent-based data exchange across institutional and national boundaries, the PoC aims to illustrate how patient empowerment and cross-border interoperability can be achieved simultaneously in the context of digital medical imaging.

In summary, the research focuses on two objectives:

- O1. To investigate the potential of blockchain, decentralised identity and off-chain storage technologies (e.g., IPFS) to enhance data integrity, consent management and user-controlled sharing in the context of medical imaging.
- O2. To develop a design-time PoC for a patient-centric imaging wallet, enabling patients to securely store, view and share imaging data across institutional and national borders, in alignment with EU standards and regulations.

These objectives are operationalised as four research questions (RQ1–RQ4) that act as design drivers for the architecture and its evaluation:

- RQ1. Are authorisation decisions for DICOMweb/FHIR requests deterministic when derived from a single live consent state?

- RQ2. Does revocation prevent valid access after a given time T in a way that can be evidenced and verified?
- RQ3. Do on-chain records remain non-identifying, avoiding the storage of personal data concerning health or stable identifiers?
- RQ4. Can an access episode be reconstructed end-to-end using standard resources (e.g., FHIR Consent, AuditEvent and Provenance) combined with non-identifying ledger anchors?

The remainder of the thesis uses these research questions to structure the architectural design in Chapters 3 and 4 and to assess whether the proposed proof of concept satisfies the intended properties of determinism, revocation, minimisation and auditability.

1.4. Contributions of this thesis

This thesis makes three main contributions. First, it proposes a standards-based conceptual architecture for a patient-centric imaging wallet that combines a permissioned blockchain, decentralised identity, and off-chain encrypted storage, explicitly aligned with DICOM/DICOMweb, HL7 FHIR, the EEHRxF, MyHealth@EU, and EU regulatory frameworks such as the GDPR, eIDAS, and the emerging EHDS. Second, it derives a set of design invariants from RQ1–RQ4 that operationalise deterministic authorisation, effective revocation, strict on-chain data minimisation and end-to-end auditability, turning the research questions into non-negotiable constraints on interfaces, data placement and governance boundaries. Third, it develops a design-time proof of concept, expressed through representative user journeys, evidence bundles and traceability mappings that link the behaviour of the imaging wallet to DICOM and FHIR artefacts and to GDPR and eIDAS obligations, demonstrating the conceptual feasibility of the approach and providing a reusable pattern for the evaluation of future implementations.

CHAPTER 2

Related Work

2.1. PRISMA Methodology

2.1.1. Information Sources

The systematic search was conducted using Scopus [20], IEEE Xplore [21], and Web of Science [22]. Scopus was selected for its broad coverage of peer-reviewed literature in health, technology and information systems, IEEE Xplore to capture technical work on secure data storage and digital health, and Web of Science to complement these with multidisciplinary coverage. Together, these databases reflect the interdisciplinary scope of this research at the intersection of healthcare, digital innovation and cybersecurity.

2.1.2. Search Strategy

To ensure a rigorous and comprehensive identification of relevant literature, a structured search strategy was developed in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines [23]. The aim was to retrieve peer-reviewed publications at the intersection of secure data storage, medical imaging, patient-managed digital health records and data governance, with particular attention to European interoperability standards and regulations.

The strategy was organised into four conceptual domains aligned with the thesis objectives: (A) data security, (B) medical imaging, (C) health data management, and (D) blockchain and interoperability, with an additional filter (E) for publication year (2020–2025) and language (English). Each domain was operationalised through representative keywords combined with Boolean OR within domains and AND across domains; the complete list of terms and domain groupings is summarised in Table 1.

Table 1 – Search Domains & keywords

Group	Conceptual Domain	Keywords / Search Terms
A	Data Security Domain	"Secure storage", "data protection", "encryption", "safeguarding", "privacy protection"
B	Medical Imaging Domain	"Medical image", "medical imaging", "healthcare imaging", "radiology", "diagnostic imaging", "health imaging"
C	Health Data Management Domain	"wallet", "personal health record", "electronic health record", "health data management", "EHR"
D	Blockchain & Interoperability	"blockchain", "decentralized storage", "distributed ledger technology", "interoperability"
E	Filter	Year (2020-2025), English

Trial searches were run iteratively across Scopus, IEEE Xplore and Web of Science [19], [21] to calibrate sensitivity and specificity. A summary of the query refinement steps and intermediate record counts is provided in Table 2.

Table 2 - Steps of document search

Search Step	Boolean Combination	Number of Records Found (Total)
A – Data Security Mechanisms	Group A only	393 298
B – Medical Imaging Domain	Group B only	1 704 936
C – Patient-Centric Records	Group C only	133 851
D – Data Governance & Interoperability	Group D only	314 558
A + B	("A" AND "B")	5 916
A + B + C	("A" AND "B" AND "C")	241
A + B + C + D	Final query: ("A" AND "B" AND "C" AND "D")	64
Final + Filter	("A" AND "B" AND "C" AND "D") AND ("E")	55

The final query applied was:

("secure storage" OR "data protection" OR "encryption" OR "safeguarding" OR "privacy protection") AND ("medical imaging" OR "healthcare imaging" OR "radiology" OR "diagnostic imaging" OR "health imaging") AND ("wallet" OR "personal health record" OR "electronic health record" OR "EHR" OR "health data management") AND ("blockchain" OR "decentralized storage" OR "distributed ledger technology" OR "interoperability")

Filtered by: Year: 2020–2025; Language: English

The final query applied the four domains jointly, restricted to 2020–2025 and English-language publications. This yielded 55 records across the three databases. After exporting to Zotero and removing 12 duplicates, 43 unique records remained. Title and abstract screening excluded 17 records that did not meet the thematic focus (e.g., not related to medical imaging, lacking a blockchain component, or not addressing secure data management), leaving 26 articles for full-text assessment. Of these, 10 were excluded due to incomplete access or insufficient alignment with the scope of this thesis, leaving 16 studies included in the final qualitative synthesis. This process is summarised in the PRISMA flow diagram in **Erro! A origem da referência não foi encontrada.**.

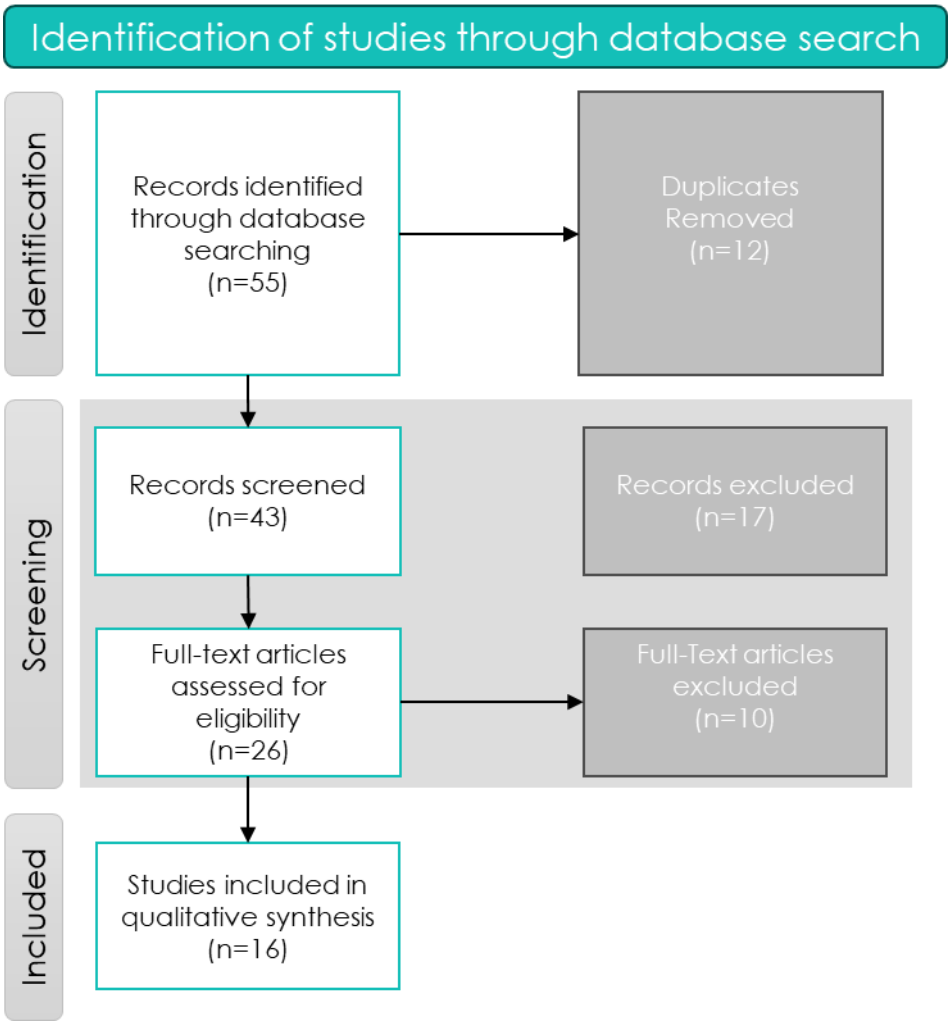


Figure 1 PRISMA of the literature review flow diagram

The 16 included studies and their main contributions are summarised in Table 3, which provides the basis for the thematic analysis developed in the remainder of this chapter.

Table 3 - Documents summary

Title	Year	Summary
Secondary Use of Electronic Health Record: Opportunities and Challenges [24]	2020	The article addresses privacy and security challenges in secondary use of EHRs, supporting the thesis's focus on secure data storage and consent management. Its analysis of GDPR and interoperability risks provides a regulatory context relevant to implementing patient-controlled wallets for medical imaging.
Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology [34]	2020	Presents a blockchain and zero trust system for secure, auditable transmission and storage of medical images using IPFS and multi-layer authentication.
A Performant Protocol for Distributed Health Records Databases [33]	2021	Describes a consensus protocol for distributed EHR systems that supports data partitioning, replication, fault detection, and compliance with data protection regulations.
Blockchain-Based Reversible Data Hiding for Securing Medical Images [37]	2021	Proposes a blockchain-integrated reversible data hiding scheme that encrypts medical images, embeds private data using histogram shifting, and ensures traceable, reversible, high-capacity secure embedding.
EHRChain: A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem [39]	2022	A blockchain/IPFS system using attribute-homomorphic encryption and fine-grained access control, optimized for secure, scalable EHR storage and sharing.

Title	Year	Summary
Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System [38]	2022	Proposes a blockchain system with attribute classification, smart contract-based access control, anonymized identities, and utility-based data matching for privacy-preserved Electronic Medical Record (EMR) sharing.
AES Encryption for Secure Storage and Transfer of Patient Health Records using Blockchain Technology [27]	2023	Combines Advanced Encryption Standard (AES) encryption with blockchain to secure storage and transfer of health records, ensuring data integrity, confidentiality, and controlled access.
Blockchain Technology for Embracing Healthcare 4.0 [30]	2023	Introduces a blockchain system for secure, real-time exchange of large health datasets, improving data integration, transparency, and confidentiality in Healthcare 4.0.
A Blockchain-Based E-Healthcare System with Provenance Awareness [29]	2024	Proposes a blockchain system with dynamic access control and traceability of medical data for secure and accountable EHR management.
A Blockchain-based PHR Sharing Scheme with Attribute Privacy Protection [28]	2024	Proposes a blockchain-based system combining zero-knowledge proofs, attribute-based access control, and encrypted off-chain storage for privacy-preserving PHR sharing.
A Multi-Layered Security Framework for Medical Imaging: Integrating Compressed Digital Watermarking and Blockchain [36]	2024	Proposes a multi-layered architecture using watermarking, encryption, and blockchain to protect medical images with integrity checks and auditable sharing.
Electronic Health Records Reimagined: A Blockchain Approach Combined with IPFS and Brain Tumor Detection Through Machine Learning [31]	2024	Presents a blockchain-IPFS system with encrypted off-chain storage and ML based brain tumor detection, ensuring data integrity, auditability, and secure imaging workflows.
HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy preserving scalable health data [35]	2024	A blockchain/IPFS framework securing encrypted health data storage and sharing, featuring metadata logging, user dashboard, and performance benchmarking.
Recommendation Systems in Healthcare: Challenges, Limitations, and Its Applications [32]	2024	Reviews healthcare recommendation systems, discussing their benefits and limitations, and emphasizes the importance of data security, privacy, and interoperability in clinical contexts.
Verified Access to EHR over Blockchain and IPFS with Lit Protocol Encryption [25]	2024	Presents a decentralised EHR system using IPFS, blockchain, and Lit Protocol for encrypted storage, verifiable access, and granular patient-controlled sharing.
MediVault DApp: A Electronic Health Record Application Using Blockchain Technology [26]	2025	Presents a blockchain-based DApp with smart contract-based access control, off-chain health data storage, and FHIR-compatible interoperability for secure EHR management.

2.2. Literature Review

The secure and interoperable management of medical imaging has become increasingly relevant in the context of digital health transformation. As European healthcare systems move toward cross-border data exchange and patient-centred care, the notion of a patient wallet, a digital tool that enables individuals to store, manage and control access to their health data, has gained prominence.

Medical imaging poses specific challenges due to its volume, sensitivity and the legal constraints surrounding its processing and sharing. Ensuring data integrity, fine-grained access control and compliance with regulatory and interoperability frameworks such as GDPR, eIDAS, FHIR and DICOM is critical.

This literature review synthesises current research that addresses these challenges through blockchain-based architectures, off-chain storage mechanisms and privacy-preserving techniques. The analysis is structured around three core dimensions: enabling technologies (Section 2.2.1), imaging-oriented use cases (Section 2.2.2) and alignment with European interoperability standards (Section 2.2.3).

2.2.1. Enabling Technologies

A substantial part of the reviewed literature focuses on technological enablers for secure, decentralised health data management, which provide the foundation for the development of patient-controlled imaging wallets. These approaches typically integrate blockchain infrastructure, off-chain storage mechanisms, and cryptographic access-control models.

Several architectures use blockchain-IPFS integration to securely and at scale handle sensitive medical data. One proposed system combines IPFS for off-chain storage of health records with a blockchain ledger that records all access transactions. It employs the Lit Protocol to enforce access control rules in a decentralised manner, allowing patients to define who can view their data without depending on any central authority [25]. Another solution, MediVault DApp, applies smart contract–based access permissions and supports FHIR interoperability, facilitating secure health data exchange between institutions and systems [26].

From a performance perspective, one study introduces a Byzantine fault–tolerant consensus protocol specifically designed for distributed EHR systems. It partitions and replicates data across nodes to enhance scalability and resilience [33].

A key thematic cluster concerns advanced encryption schemes. In EHRChain, attribute-based encryption and a homomorphic cryptosystem enable fine-grained access control, while also allowing privacy-preserving data operations and external auditing [39]. Another work introduces a privacy-preserved EMR exchange model using smart contracts and anonymised identities to implement dynamic and secure sharing logic [38].

Other contributions highlight infrastructure-level interoperability and real-time scalability. For example, HealthRec-Chain integrates metadata logging, encryption, and a user-facing dashboard to support fault-tolerant, patient-centric data workflows [35]. Likewise, Blockchain Technology for Embracing Healthcare 4.0 proposes a modular blockchain framework to address the fragmentation of data across systems and support synchronised health data sharing in large-scale networks [30].

2.2.2. Imaging-oriented use cases

Several of the reviewed studies focus specifically on the management of medical imaging data, addressing its unique technical and regulatory demands. These works recognise the challenges associated with large file sizes, sensitive clinical content, and the need for secure, traceable, and compliant sharing mechanisms. In response, various authors propose adaptations of blockchain

infrastructures, often combined with off-chain storage and image-level protection techniques, tailored to the secure handling of diagnostic imaging within decentralised environments.

Some studies highlight the security of images using combined cryptographic and blockchain mechanisms. One such approach integrates AES encryption with blockchain to secure the storage and transfer of patient health records. By encrypting medical images before anchoring their metadata on-chain, the system ensures the confidentiality, integrity, and auditability of image exchanges between institutions [27]. Another architecture employs digital watermarking, combined with encryption and blockchain, to embed traceable metadata directly into medical images. This method provides enhanced protection for ownership verification and tamper detection, while preserving image quality [36].

A further solution explores reversible data hiding within encrypted medical images using histogram shifting. Blockchain is used to store cryptographic hashes of the original image and embedded content, enabling verifiable, traceable, and fully reversible modifications [37].

In terms of architecture, several contributions recommend separating the storage and control layers. One example combines IPFS for storing encrypted medical images off-chain with blockchain access management and origin tracking. The system was developed in the context of AI-assisted brain tumour detection, yet its infrastructure can be extended to broader medical imaging workflows [31].

Security policies are also reinforced through decentralised trust models. One proposal adopts a zero-trust security framework, integrating public key encryption, device verification, and access enforcement within a blockchain system for image sharing. This approach ensures that only authorised devices and identities can request or retrieve sensitive imaging data, a critical feature for distributed healthcare networks [34].

Taken together, these imaging-oriented studies reflect a growing recognition of the distinct requirements posed by diagnostic image data. Their proposed solutions vary in method, ranging from encryption and watermarking to off-chain distribution and multi-factor verification, but converge around the goal of ensuring confidentiality, integrity, and regulatory compliance in decentralised imaging environments.

2.2.3. Interoperability and Compliance

Ensuring interoperability and regulatory compliance remains a central concern in the implementation of blockchain-based health data systems, particularly in contexts involving cross-border exchange, patient sovereignty, and compliance with European legal frameworks

such as GDPR, eIDAS, FHIR, and DICOM. Several studies in the reviewed literature directly address these dimensions, highlighting both architectural adaptations and policy design considerations.

One study examines the secondary use of EHRs and the accompanying risks of data misuse, especially in systems where patient consent is poorly integrated, or data exchange is not tightly governed. The paper emphasises the need for consent enforcement mechanisms, traceable access control, and alignment with GDPR principles, positioning these requirements as essential for implementing trustworthy patient-managed systems as wallets [24].

Other work explores how blockchain architectures can reinforce compliance by maintaining immutable records of data origin, access, and modification. One such system uses a Directed Acyclic Graph (DAG) ledger and smart contracts to dynamically adjust access policies based on the origin of the health data. This enhances transparency, accountability, and auditability in healthcare data workflows [29].

Efforts to design privacy-preserving sharing strategies also integrate regulatory concerns into technical choices. For example, one architecture combines zero-knowledge proofs, attribute-based access control, and encrypted off-chain storage, ensuring that access can be restricted not only by user identity but also by attribute-level [28]. This approach supports patient-controlled consent enforcement while remaining compatible with data minimisation and purpose limitation obligations under European law.

Finally, one article reviews the state of healthcare recommendation systems and points out systemic limitations in data governance, system integration, and trust frameworks. Although not blockchain-specific, the study underlines the structural importance of standardised interfaces, interoperable data models, and secure identity management, all of which remain relevant to the deployment of medical imaging systems under EU interoperability goals [32].

Collectively, these studies underline that technological robustness alone is insufficient without policy-aware design. As medical imaging systems become more distributed and patient-driven, compliance with European interoperability and data protection frameworks must be embedded at both the infrastructure and governance layers of system design.

2.2.4. Gaps in the Literature and Research Opportunity

While the literature demonstrates significant progress in applying blockchain technologies to health data management, several limitations remain unaddressed, particularly in the secure and interoperable handling of medical imaging data. The reviewed studies present robust

approaches to encryption, off-chain storage, and smart contract–based access control; however, most of these systems either generically treat health data or focus narrowly on EHRs, with limited attention to the unique characteristics and requirements of imaging records.

Specifically, few works explicitly consider medical imaging standards such as DICOM, nor do they offer detailed strategies for managing large, high-resolution image files within blockchain environments. Although some studies use IPFS or other distributed storage systems, integrating these systems with imaging-specific metadata, formats, and compression protocols remains underexplored.

Moreover, while regulatory compliance is frequently mentioned, the degree of alignment with EIFs, including GDPR, eIDAS, FHIR, and MyHealth@EU [40] varies considerably. Most solutions embed generic data protection mechanisms, but few provide mechanisms for cross-border data portability, consent traceability, or patient sovereignty that are directly compatible with EU policy goals. Patient-managed access is often mentioned but not operationalised through interfaces that reflect real-world health governance requirements.

Considering these gaps, this thesis proposes a secure, blockchain-based architecture for managing medical imaging in a patient-controlled wallet, explicitly grounded in European interoperability and data protection standards. By combining imaging storage strategies with granular consent enforcement and legal compliance by design, the proposed solution aims to fill a critical niche in the current landscape of digital health infrastructure.

2.3. World Case Review: Real-World Implementations of Blockchain in Health Data Management

Moving beyond academic research, examining real-world implementations provides valuable insights into the feasibility, effectiveness, and practical challenges of blockchain-based health data management solutions. Several prominent cases illustrate how blockchain technology is being leveraged to enhance the security, traceability, and interoperability of health data, particularly in the European context.

Estonia’s national health infrastructure is widely recognised as one of the earliest and most mature implementations of blockchain in public healthcare. Since 2016, the country has integrated blockchain into its EHR system using the Keyless Signature Infrastructure (KSI Blockchain) [41], a technology developed by the Estonian company Guardtime. Rather than storing medical records directly on-chain, the system generates cryptographic hash values from

EHR activity. It records them on the blockchain, ensuring tamper-evident verification of access and modification events [42].

The blockchain operates in conjunction with Estonia's X-Road [43], interoperability framework, which securely connects over 1,000 public and private services, including hospitals, general practitioners, and pharmacies [42]. This infrastructure enables real-time exchange of health data while allowing patients to monitor who accessed their records, when, and under what legal basis. Patient data sharing and access permissions are tightly governed by the Estonian digital ID system, with consent mechanisms that align with the GDPR and eIDAS Regulation. Estonia's architecture demonstrates that blockchain auditability, data integrity, and patient transparency can be achieved at a national scale while fully complying with EU standards.

The PharmaLedger project is a large-scale European initiative that exemplifies the potential of blockchain for trusted health data exchange across borders [44]. Funded by the European Union's Horizon 2020 programme [45] and supported by the Innovative Health Initiative (IHI) [46], the project brings together over 29 partners, including pharmaceutical companies, hospitals, academic institutions, and technology providers, to co-develop blockchain tools for the healthcare sector [44]. Its use cases include clinical trial data integrity, product traceability, and electronic Product Information (ePI), all of which are designed to comply with EU data protection frameworks such as GDPR and eIDAS.

A central aspect of PharmaLedger is its commitment to interoperability, demonstrated by adopting FHIR standards for health data exchange and by designing modular, open-source components that can be adapted to national infrastructures. The project explicitly promotes patient-centric governance, proposing blockchain consent models that allow individuals to grant, revoke, or delegate access to health data in a transparent and auditable manner [44]. While not explicitly focused on medical imaging, the project provides concrete evidence that standardised, privacy-compliant, and interoperable blockchain systems can be designed for cross-border healthcare scenarios within the EU.

From a global perspective, BurstIQ in the United States provides another practical use case, particularly relevant for its data exchange model, smart contract consent management, and compatibility with healthcare interoperability standards. BurstIQ implements blockchain technology to securely manage and share sensitive healthcare data among patients, healthcare providers, and research institutions. Its platform integrates decentralised storage models, robust encryption, and detailed audit trails, effectively demonstrating the scalability and practical feasibility of blockchain-enabled patient-controlled health records [47].

Reflecting on these real-world examples highlights critical factors influencing the successful deployment of blockchain solutions: strong regulatory alignment, integration with established healthcare standards (e.g. FHIR and DICOM), and a patient-centric approach to data governance.

These insights collectively inform the direction of this thesis, which seeks to address the gaps identified by proposing an architecture tailored explicitly for secure and patient-controlled medical imaging storage, fully aligned with EIFs and compliance requirements.

CHAPTER 3

Conceptual Architecture and Compliance Baseline

3.1. Methodological Approach and Scope

This study uses the Design Science Research Methodology (DSRM [48]), which offers a framework for problem identification, solution design, and evaluation. Chapters 1 and 2 address the first two steps. This chapter focuses on step three, the conceptual architecture of the imaging wallet. The subsequent chapters instantiate the design and evaluate it through analytical validation rather than empirical testing.

3.1.1. Research questions as design drivers

In this scenario, the research questions are treated as design drivers that constrain interfaces, data placement, governance, and verifiable outputs, as formulated in Chapter 1 (RQ1-RQ4). Alongside the research questions, the design invariants that must be maintained for the architecture to be valid, the architectural levers that enforce these invariants, and the evidence presented in Chapter 4 to prove conformance at design time are also part of the design. Table 4 summarises this operationalisation of RQ1–RQ4.

Table 4 - Operationalising RQ1–RQ4 as design drivers

RQ	Design invariant (must hold)	Architectural levers (how it is enforced)	Evidence hook (what is demonstrated in Chapter 4)
RQ1	A single live consent state determines every DICOMweb/FHIR request; there is no alternative path that bypasses it.	Access gateway mediates all DICOMweb/FHIR calls; consent contract on a permissioned ledger; deny-by-default in ambiguous cases; short-lived, audience-bound tokens with optional proof-of-possession; FHIR Consent as a policy reference; provider identity via DID and Verifiable Credentials (VCs) at eIDAS-aligned assurance.	Allow/deny outcomes tied to the same consent state; token issuance log reflecting scope, audience, and Time-To-Live (TTLs [49]; gateway decision trace; AuditEvent entries for both allow and deny.
RQ2	After revocation time T, all subsequent requests are denied within a bounded propagation window.	Revocation semantics encoded in smart contracts; gateway re-checks consent on every request or uses ultra-short token TTL; cache invalidation rules; quorum finality; qualified time reference where applicable.	On-chain revocation tx ID and time reference; first deny no later than T + bound; post-T deny AuditEvents; documented token TTL/introspection settings.
RQ3	No clinical pixels, stable identifiers, or resolvable content addresses are recorded on-chain; only non-identifying commitments and policy states appear.	Salting per object and per policy state; pseudonymous handles; pointer/key rotation; FHIR AuditEvent/Provenance kept off-chain; on-chain schema restricted to digests and state.	On-chain field schema snippet; worked example of digest construction; data-flow showing off-chain placement; DPIA sketch cross-reference.
RQ4	Any access episode can be reconstructed end-to-end using standard resources without exposing pixel data.	Emission of FHIR AuditEvent and Provenance for all decisive actions; stable correlation keys; OperationOutcome for errors; exportable, signed evidence bundle.	Timeline reconstruction for an episode; link set across Consent/Provenance/AuditEvent; signed evidence bundle containing request_id, purpose_code, decision, and consent_state_hash.

Considering everything, RQ1–RQ4 limit the architectural baseline by mandating a single authorisation plane that interfaces with DICOMweb and FHIR. These tokens are either introspected or have a short lifespan with precise revocation semantics, a separation between on-chain policy facts and off-chain clinical content, and standards-based observability using FHIR Consent, AuditEvent, and Provenance. Chapter 4 uses these drivers again to define artefacts and success criteria for journeys J1–J4, ensuring that each RQ is supported by tangible artefacts rather than by execution metrics.

3.2. Functional and Non-Functional Requirements

Research goals, stakeholder needs, and the regulatory context guide both the functional and non-functional requirements that the imaging wallet's design must address. Examples of functional requirements include secure image storage, permission management, and international data transfer. Non-functional requirements specify the operational constraints and quality attributes that these functions must meet, such as compliance, scalability, security, and usability. Taken together, these specifications lay the groundwork for the system's design, ensuring that the wallet meets both technical feasibility and the expectations of European standards and patients.

3.2.1. Functional Requirements

Alignment with EIFs, strong authentication and identity management, cross-border sharing, transparency, granular and revocable consent, and secure image management are functional requirements for the imaging wallet. These requirements are consolidated in Table 5, which also provides the identifiers used in the architectural and compliance mapping that follows.

Table 5 - Functional requirements of the imaging wallet

ID	Requirement	Description
FR-01	Secure Image Management	Patients must be able to upload, store, view, and download medical imaging files in standard formats (e.g., DICOM), ensuring portability and interoperability across healthcare systems.
FR-02	Granular Consent Management	Patients must control access to specific images, granting, denying, or revoking permissions in a fine-grained and traceable manner, in line with GDPR requirements.
FR-03	Cross-Border Sharing	The system must enable the sharing of imaging data across EU Member States, using interoperability standards such as DICOM and FHIR to ensure seamless integration.
FR-04	Auditability and Transparency	All access and sharing events must be immutably recorded on the blockchain, enabling patients and regulators to verify compliance and accountability.
FR-05	Secure Authentication & Identity Management	Access to the wallet must be based on robust identity verification for patients and healthcare providers, using national electronic identity or DIDs in compliance with eIDAS.
FR-06	Interoperability with European Standards	The system must comply with EU-level frameworks such as EEHRxF, EHDS, and EIF, ensuring consistent, secure, and lawful data exchange across Member States.

3.2.2. Non-Functional Requirements

Regulatory, technical, and quality expectations are reflected in the non-functional requirements. These include processing that complies with the GDPR, adequate performance for time-sensitive clinical workflows, strong data integrity and security under patient-centred key control, scalability for large imaging workloads, reliability and high availability comparable to clinical systems, and usability and accessibility for diverse patient populations. These needs and the identifiers mentioned later in the evaluation and design are summarised in Table 6.

Table 6 – Non-functional requirements of the imaging wallet

ID	Requirement	Description
NFR-01	GDPR Compliance	Encrypted storage, logged consent, and support for GDPR rights (withdrawal, portability, erasure) ensure lawful processing of patient data.
NFR-02	Scalability	Off-chain storage and horizontal scaling enable the system to handle large volumes of data and users without compromising performance.
NFR-03	Interoperability	Adopts standards (DICOM, HL7 FHIR) and frameworks (EEHRxF, MyHealth@EU) to ensure cross-border semantic and legal compatibility.
NFR-04	Availability & Reliability	Decentralised architecture ensures redundancy, >99.9% uptime, and recovery mechanisms in the event of outages or device loss.
NFR-05	Data Integrity & Security	Images are protected by encryption (AES-256) and verified by on-chain hashes, with keys controlled exclusively by patients.
NFR-06	Usability & Accessibility	Intuitive, multilingual, mobile-friendly, and compliant with accessibility guidelines (e.g., WCAG) to ensure broad adoption.
NFR-07	Performance & Response Time	Upload, retrieval, and sharing of imaging files must remain fast and reliable to avoid delays in clinical workflows.

Design-time service assumptions. In the absence of empirical benchmarking, design is guided by qualitative expressions of performance and availability: routine workflows should complete CT Scan and MRI study transfers within clinically acceptable windows; consent interactions should have a short user-interaction cycle; and the audit and consent plane should maintain high availability with rapid recovery. These assumptions inform the sizing, caching, and replication strategies. Empirical benchmarking is out of scope for this dissertation and is identified as future work.

3.2.3. Design-time assumptions and constraints

The architecture is developed under the following explicit assumptions and constraints to ensure clarity and control over scope. The following design-time constraints and assumptions are reviewed in Chapter 4 and summarised in Appendix C, Table 23, which covers identity and

trust, governance, data placement, interoperability, authorisation, security, availability, compliance, and implementation neutrality.

Violations of these assumptions have clear operational implications. Without high-assurance identification, cross-border portability may be compromised by the need for additional verification steps or lower-assurance fallbacks. If ledger finality exceeds the assumed bound, the revocation propagation window may expand, and the gateway is designed to default to denial in such cases. If partners omit standard AuditEvent entries, audit reconstruction remains possible but is flagged as partial, with on-chain anchors still providing policy provenance.

The module boundaries specified in Section 3.3 and the evaluation guidelines utilised in Chapter 4 are shaped by these presumptions and constraints. Without overcommitting to deployment-specific details, they maintain the artefact's ability to be implemented, to preserve privacy, and to comply with European interoperability standards.

3.3. Reference layered model and architectural baseline.

To meet the specified requirements, the proposed system uses a modular, patient-centric architecture that incorporates blockchain, decentralised identity, and off-chain storage. The primary aim is to give patients sovereign control over their medical images while facilitating safe, standards-compliant access for healthcare providers. The solution is organised into interoperable layers and modules in line with the EIF's modularity principle to support fault isolation, reusability, and smooth integration with the larger EHDS [4].

The solution uses HL7 FHIR for metadata and compliance evidence, and DICOMweb for imaging operations to operationalise interoperability [18], [50]. While FHIR ImagingStudy and DocumentReference facilitate indexing and discovery across institutions, Query based on ID for DICOM Objects using Restful Services (QIDO-RS), Web Access to DICOM Objects using RESTful Services (WADO-RS) and Store Over the Web using RESTful Services (STOW-RS) are used for querying, retrieval, and storage [18], [50]. FHIR Consent, Provenance, and AuditEvent are used to express patient directives, lineage, and audit [18]. This interface profile offers semantic and legal compatibility for cross-border use by aligning with EEHRxF datasets and the services available through MyHealth@EU [1], [3], [15], [40].

User Layer. The Patient Wallet Module, a mobile or web application at the top of the architecture, allows users to manage keys and consent choices, as well as to upload, view, and share encrypted imaging data. The wallet protects usability and patient sovereignty over medical data by providing a straightforward interface that abstracts technical complexity.

Identity Layer. The DID Services Module manages verifiable credentials and authentication. It creates and validates DIDs, issues credentials in accordance with eIDAS and the W3C DID/VC specifications and ensures that healthcare providers and patients are authenticated using reliable methods. This module enables secure cross-border identity management and connects the system to the upcoming EUDI Wallet.

Data Layer. Large, encrypted imaging files, usually in DICOM format, are stored under the Off-Chain Storage Module's control. Files are encrypted locally and stored in distributed repositories such as IPFS or EU-resident cloud storage to ensure scalability and GDPR compliance. Each file is identified by a cryptographic hash, which is stored on the blockchain for validation. This approach ensures integrity and security without overloading the ledger.

Logic and Consensus Layer. The Blockchain Network Module serves as the coordination and trust layer. It provides auditability, uses smart contracts to enforce patient-defined access policies, and permanently records metadata and consent decisions. The network, which operates as a permissioned ledger (e.g., Hyperledger Fabric or Besu), is overseen by regulators and certified healthcare organisations, ensuring accountability and adherence to GDPR, European Telecommunications Standards Institute (ETSI [51]) trust standards, and the European Blockchain Services Infrastructure (EBSI [52]) framework [5]. To comply with European data protection regulations and safeguard the security and privacy of sensitive healthcare data, a permissioned ledger was selected over a public ledger, as permissioned models allow controlled participation and governance mechanisms suitable for regulated environments [53]. A permissioned ledger limits access to reliable, accredited healthcare organisations and regulatory bodies, ensuring that only authorised entities can interact with consent data and audit records, in contrast to public ledgers that permit any participant to write to the ledger [54]. Furthermore, by ensuring that only non-identifying information is entered into the ledger and adhering to data minimisation principles, this decision protects patient control over their data and guards against unauthorised access or alteration [54].

Integration Layer. The architecture connects to clinical systems and external healthcare providers via the Access Requester Interfaces Module. Hospitals and clinics can request imaging data, verify patient consent against blockchain records, and retrieve encrypted files from storage using HL7 FHIR and DICOMweb application programming interfaces (APIs).

This ensures semantic alignment with EEHRxF datasets and interoperability with national infrastructures and the MyHealth@EU framework.

Operations Layer. The Resilience and Monitoring Module ensures reliability and service continuity. To meet clinical-grade uptime goals, it uses redundancy, observability, and automated recovery, aligned with ISO 27001/27701 [55], [56] and Site Reliability Engineering practices.

Security Layer. Several cross-cutting modules strengthen trust and compliance. The Audit and Provenance Module enables transparency for patients and regulatory oversight, providing immutable records of every action. By issuing temporary tokens compliant with Open Authorization (OAuth [57]) 2.1, User-Managed Access 2.0 (UMA [58]), and OpenID Connect (OIDC [58]), the Access Gateway Module connects blockchain-based consent with traditional authorisation flows, ensuring that access to imaging data remains in line with the patient's preferences. In line with recommendations from the European Union Agency for Cybersecurity (ENISA [59]), the Cryptographic Services Module ensures confidentiality and integrity by providing encryption, decryption, hashing, and secure key management across all layers.

The ledger adheres to data minimisation and privacy-by-design principles. Unique identifiers and personal information are not stored on the chain. Rather, the chain uses salted cryptographic digests of content addresses and policy states to store non-identifying commitments to off-chain artefacts. Instead of modifying historical blocks, state modifications and key invalidation are used to enforce consent revocation. Stale references are rendered unusable by pointer rotation and key lifecycle controls, aligning immutability with the GDPRs minimisation and erasure requirements.

Actors and roles. Through the Wallet Module, the patient exercises sovereign control over consent, keys, and imaging data. Through the Integration Layer, healthcare providers request access, authenticate using an eIDAS-aligned identity, and obtain time-bound authorisation from the Access Gateway. Accredited healthcare organisations and competent authorities that run the permissioned ledger in the Logic and Consensus Layer are known as consortium validators. eIDAS-compliant identity providers and trust service providers that interface with the Identity Layer offer qualified trust and identity services. Under data-processing agreements, storage node operators host EU-resident repositories in the data layer. Audit and Provenance outputs are used for oversight by regulators and auditors. This role mapping clarifies accountability without changing the previously mentioned patient-centric control model.

The architecture is organised into layers of interoperable modules, each of which oversees a specific set of tasks, as shown in Figure 2. Dashed arrows indicate auxiliary services such as

auditing, cryptography, and monitoring, while solid arrows indicate patient-initiated data and consent flows.

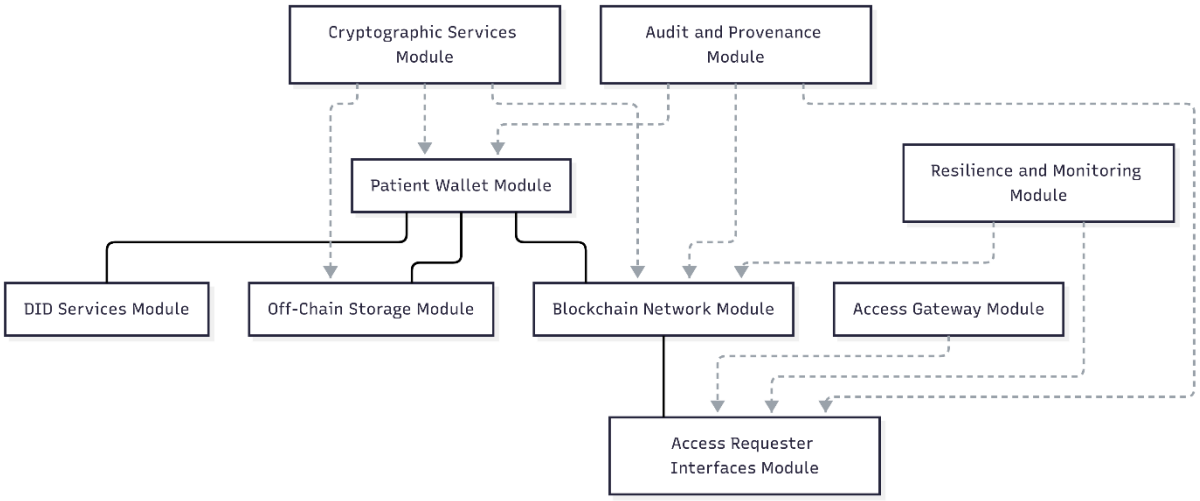


Figure 2 – Modular high-level conceptual architecture of the patient imaging wallet.

The Patient Wallet, DID Services, Off-Chain Storage, Blockchain Network, and Access Requester Interfaces are the core modules of the layered modular design shown in the figure. Cross-cutting modules for auditing, authorisation, cryptography, and resilience are also included. Appendix C, Table 24 provides a detailed mapping of these modules to specific technology classes, relevant standards, and illustrative implementation options. To demonstrate that the modular design is implementation-neutral while adhering to European interoperability and compliance frameworks, the table lists the primary technology families (such as DLT platforms, off-chain storage, identity and trust services), the corresponding interoperability standards (such as DICOM, FHIR, EEHRxF, MyHealth@EU, and eIDAS), and sample solutions for each architectural module.

The architecture's value lies not only in its layered structure but also in the practical interactions between its modules. Under the GDPR, patient-initiated information flows are controlled by explicit consent, promoting privacy by design. The image-upload process from wallet to off-chain storage and ledger is depicted in Figure 3, where a single patient-initiated flow combines authentication, client-side encryption, storage, integrity and consent anchoring, and audit logging.

Patient control and consent are central to data sharing. Figure 3 illustrates the workflow: a healthcare provider submits a standards-based request through the integration interfaces; consent is checked against the ledger and, when required, confirmed by the patient via the wallet; and the access gateway issues a short-lived token authorising retrieval of encrypted imaging data from off-chain storage. Each step is recorded as a FHIR AuditEvent.

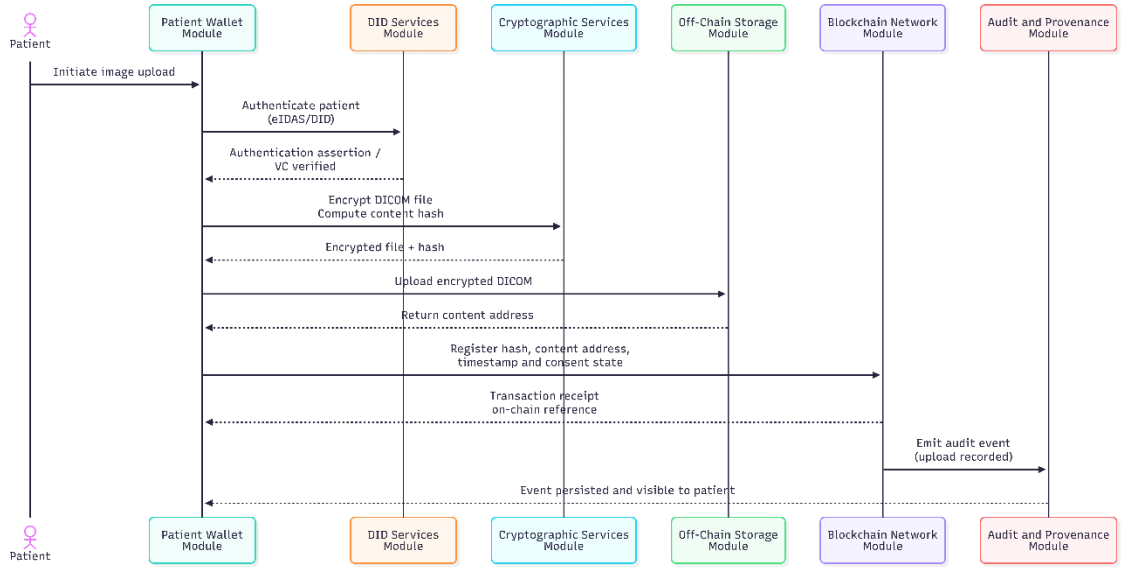


Figure 3 – Image upload sequence from wallet to off-chain storage and ledger.

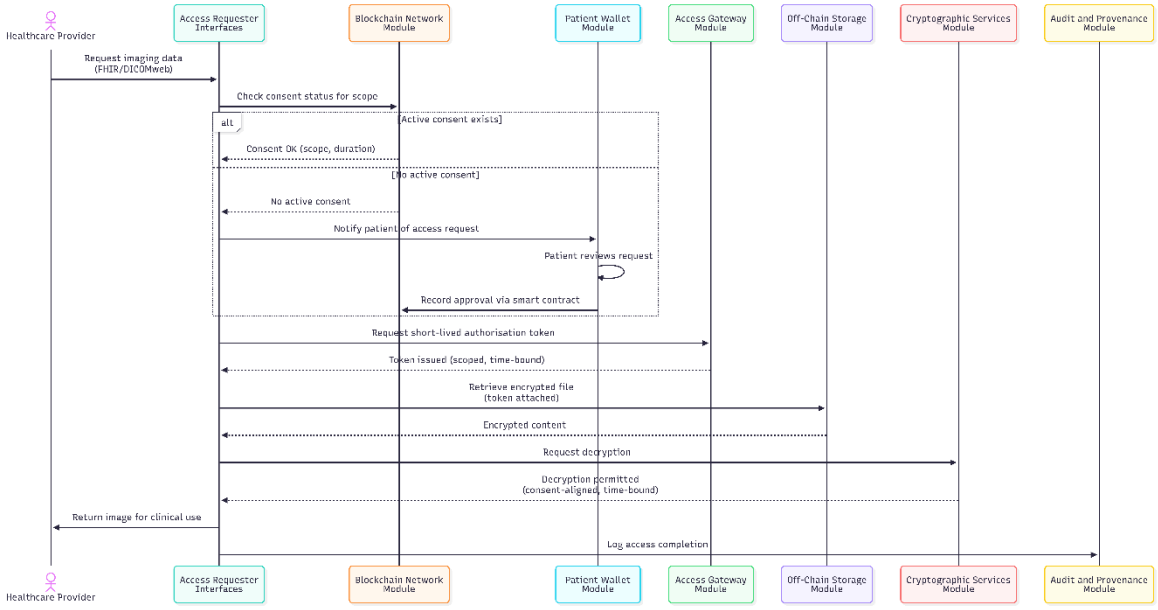


Figure 4 – Data sharing sequence for the patient imaging wallet.

The architecture achieves Objective 1 by combining standards-based interfaces, privacy-preserving consent enforcement, and verifiable audit within a patient-controlled wallet. By documenting a PoC that exercises the DICOMweb and FHIR interfaces end-to-end and confirms compliance with the compliance mapping through analytical evaluation, Chapter 4 advances Objective 2.

3.3.1. Architectural Decision Record summary

Lightweight Architectural Decision Records (ADRs) document the architectural decisions that underpin the design. This allows each non-obvious decision to be clearly stated, its justification to be seen, and its effects on requirements and evaluation to be tracked. Appendix B Table 22, Lists deferred topics, left for implementation-time validation without undermining the current argument, while Appendix B Table 21 Summarises the ADRs on which the rest of the design is based. Taken together, these documents provide a clear connection between the evaluation lenses in Chapter 4, the modular architecture in Section 3.3, and the requirements in Chapter 2.

A few key architectural choices form the foundation of the design and influence all other elements and flows. To ensure authorisation outcomes and revocation effects are deterministic and independent of long-lived artefacts, consent is continually assessed at the time of the request against a single live state [ADR-01]. A permissioned consortium ledger, run by accredited healthcare organisations, serves as the foundation for consent and audit states [ADR-02], prioritising governed trust and accountability over anonymous public mining. Only salted commitments and policy states are written to the ledger [ADR-03] [ADR-04]. DICOM objects are stored in encrypted off-chain repositories within the EU, and clinical pixels and directly identifying attributes never appear on-chain. The solution is anchored in widely accepted European interoperability profiles. It avoids custom interfaces by limiting all external interactions to DICOMweb for imaging operations and HL7 FHIR for metadata, consent, and audit [ADR-06].

3.3.2. Interface profile anchors

The conceptual architecture described above is implemented using a purposefully limited set of standardised interfaces that serve as profile anchors for the rest of the thesis. For imaging, the solution uses DICOMweb as the sole interface family for pixel operations: QIDO-RS for querying imaging studies and series, WADO-RS for retrieval, and STOW-RS for upload when necessary. This ensures that any PoC implementation can be integrated with current PACS and

Vendor Neutral Archive (VNA [60]) deployments without altering their internal data models, and that the wallet, storage services, and clinical systems communicate through widely used, HyperText Transfer Protocol (HTTP [61]) based services rather than proprietary protocols.

The architecture uses Representational State Transfer (REST [62]) operations and HL7 FHIR resources for metadata, consent, lineage, and audit. ImagingStudy and DocumentReference provide discovery and indexing of off-chain DICOM objects; the canonical representation of patient directives and policy states is Consent; Provenance captures the derivation of artefacts; and AuditEvent records security-relevant actions along the access path. FHIR OperationOutcome is used to communicate error semantics and validation feedback. These resources align with the profiles and datasets required by MyHealth@EU and the EEHRxF, enabling payloads to be transferred between national contact points without custom transformation.

Widely used web security profiles form the foundation for identity and authorisation flows. Clinical systems and, when appropriate, a UMA style of token delegation are exposed to OAuth 2.1 and OIDC endpoints via the access gateway, constantly in a way that binds issued tokens to the consent state documented on the permissioned ledger and to high-assurance organisational identities under eIDAS. Rather than introducing any new cryptographic primitives or protocol extensions, the thesis defines a conservative interoperability profile that serves as a benchmark for both the journey-level evaluation in Chapter 4 and the conformance mapping in Section 3.4.

3.3.3. Governance preview

The architecture's reliability depends not only on technical controls but also on the governance arrangements of the consortium that runs it, since the ledger supporting consent and audit is permissioned rather than public. This subsection outlines the governance baseline assumed by the design and made clear in the ADR-02 and ADR-11. Still, it does not specify a particular legal form or contractual framework.

Validators are intended to be competent, accredited healthcare organisations that meet the requirements set out in a published consortium charter. Operational incidents, parameter modifications, and membership decisions are documented and subject to change-control protocols. Supermajority consensus enables the timely completion of consent and revocation transactions, even with a limited number of invalid or unavailable validators. To confirm adherence to sectoral requirements arising from the EHDS and GDPR accountability

obligations, independent audit bodies, such as mandated third parties or supervisory authorities, have read access to on-chain state and related evidence.

A few non-functional requirements are supported and constrained by these governance presumptions. Independent auditing, transparent membership regulations, and high-assurance validator identity support trust in the accuracy and immutability of consent and audit records. The service-level goals outlined later in this chapter are informed by supermajority finality, which limits the revocation propagation window on which RQ2 depends. One of the residual risks considered in the Data Protection Impact Assessment (DPIA) sketch and risk analysis in Chapter 4 is validator misbehaviour, which can be managed through clear incident-handling and oversight procedures. The preview offered here is sufficient to evaluate architectural viability and regulatory plausibility at design-time, but the specific instantiation of governance is left to future implementation work.

3.4. Standards and Legal Compliance Mapping

This section links the system's functional and non-functional requirements to the main European standards and legal instruments governing identity, security, interoperability, and cross-border exchange, building on the modular architecture described in Section 3.3. Each requirement is mapped to the relevant GDPR and eIDAS provisions and to the FHIR, DICOM/DICOMweb, and EEHRxF anchors that guide implementation choices and design-time evaluation, consolidated in Appendix A, Table 20.

EEHRxF aligns these standards for portability within MyHealth@EU and the EHDS; eIDAS, including the EUDI Wallet framework, supports high-assurance identification and, where applicable, trust services; FHIR and DICOM/DICOMweb provide the interoperability substrate for metadata and imaging exchange; and the GDPR frames lawful and accountable processing, explicit and revocable consent, auditability, and resilience. For later prototype validation, Appendix A, Table 20 can be used as a checklist against the mapped legal and interoperability anchors.

3.4.1. Conformance and verification hooks

In addition to being descriptive, the compliance matrix in Section 3.4 outlines the verification hooks used in the analytical assessment. Each mapped capability and quality attribute is linked to one or more standards, laws, and architectural elements; these links constitute obligations that subsequent design artefacts must meet. These hooks are instantiated at design time in

Chapter 4 through the user journeys, minimal evidence bundle, and traceability matrices. They identify the specific FHIR and DICOM resources, ledger entries, and audit records that would prove conformance for each research question, as well as the circumstances in which a violation would be detectable. This arrangement provides a clear path for future empirical validation. It enables the proof of concept to be evaluated against GDPR, eIDAS, EEHRxF, and related frameworks without running a live system.

3.5. Chapter summary and transition

The conceptual architecture and its regulatory anchors are established under explicit design-time constraints in Chapter 3. Consent, identity, audit, and interoperability responsibilities are organised according to the research questions. While maintaining cross-border portability and privacy by design, the architectural choices and interface anchors keep the design feasible. These design commitments are carried over into a PoC in Chapter 4, where they are assessed using verifiable artefacts, user journeys, and success criteria.

CHAPTER 4

Proof-of-Concept Design and Evaluation Method

4.1. Purpose and scope

A design-time PoC blueprint for a patient-centric imaging wallet, translating the thesis goals into tangible elements, data flows, and verification artefacts. It instantiates the conceptual architecture, the functional and non-functional requirements, and the ADR-01–ADR-13 in accordance with the GDPR, the eIDAS framework, the developing EHDS, and the EEHRxF/MyHealth@EU profiles for cross-border exchange.

In contrast to the complete deployment of national infrastructures or live integrations with national contact points, the proof of concept is deliberately limited to the medical imaging end-to-end authorisation and audit path. The emphasis is on how consent is expressed, assessed, revoked, and demonstrated across the wallet, gateway, ledger, and off-chain storage, and on how these actions can be analytically justified. The focus is on deterministic allow and deny decisions under DICOMweb and FHIR (RQ1), effective revocation with a bounded propagation window (RQ2), strict data minimisation for on-chain content (RQ3), and reconstructable audit narratives (RQ4), in line with the design choices recorded in [ADR-01–ADR-13].

A design-time approach, specifying user journeys, success criteria, and evidential artefacts rather than runtime measurements to keep the evaluation manageable without execution. The privacy and governance restrictions encoded in [ADR-02] [ADR-03] [ADR-04] [ADR-08], and the standards and profiles presented in Chapter 3, form the foundation for verification. [ADR-11], [ADR-12], and [ADR-13] also address how these artefacts align with the research questions RQ1–RQ4. For image operations, API interactions remain anchored in DICOMweb; for metadata, consent, provenance, and audit, they are anchored in FHIR.

No particular vendor stack or ledger runtime is recommended, and performance benchmarking, scalability testing, or usability trials are out of scope. Production-grade operational playbooks, hospital PACS/VNA configuration, and national connector details are not covered. These omissions, which are apparent limitations, are discussed under findings, open issues, and validity. The goal is to produce a defensible artefact-level design that is transparent enough to support critical evaluation in the absence of a working prototype, precise enough to implement, and constrained sufficiently to meet European compliance and interoperability expectations. To answer RQ1–RQ4 without running a system, the artefacts described here provide the foundation.

4.2. Conceptual architecture

This section describes the high-level architecture of the patient-centric imaging wallet PoC. Under explicit legal and interoperability assumptions, it realises the conceptual model from Chapter 3 as a set of components, interfaces, and trust boundaries that implement the recognised ADRs. While maintaining implementation neutrality, the description defines the roles of the wallet, access gateway, permissioned ledger, off-chain encrypted storage, identity providers, and interoperability endpoints, so that later-defined user journeys and evidential artefacts can be linked to design decisions.

4.2.1. Actors and Trust Boundaries

The actor set presented in Section 3.3 (patients, healthcare providers, wallet and gateway operators, data custodians such as hospitals and VNAs, identity and trust services, consortium validators, auditors, and regulators) is reused in the PoC. These actors are grouped into four primary trust boundaries for security and accountability:

- the patient boundary, covering the wallet, its key material, and the patient's device.
- the clinical boundary, covering provider systems that consume FHIR/DICOMweb and rely on the gateway for authorisation.
- the infrastructure boundary, covering off-chain encrypted storage, interoperability endpoints, and operational monitoring.
- the consortium boundary, encompassing the permissioned ledger and its governance.

While imaging data confidentiality is maintained at the boundary between patient devices, storage services, and clinical systems, patient consent is enforced at the edge of the boundary between the clinical and consortium domains by the access gateway. Appendix C, Table 25 provides a more detailed mapping of individual roles to trust boundaries.

4.2.2. Key Layers of the Architecture

The architecture comprises five functional layers, each overseeing tasks that support cross-border interoperability and safe, patient-controlled data management. An outline of each layer's responsibilities is provided in Table 7.

Table 7 – Key Layers of the Architecture

Layer	Description
Patient Interface Layer	The web and mobile front ends allow patients to upload imaging data, view metadata, audit history, and manage consent actions (e.g., share, update, suspend, revoke). The interface only exposes the data and actions permitted by the patient's current consent state.
Access and Authorisation Layer	This layer handles identity and access management using decentralized identifiers and verifiable credentials. It translates the patient's consent state into request-time authorization, issuing short-lived tokens with explicit scope, audience, and expiration, while validating provider attributes and roles.
Data Storage Layer	Off-chain encrypted storage holds DICOM images and metadata, accessed via DICOMweb protocols (QIDO-RS, WADO-RS, STOW-RS). Only non-identifying metadata is stored on-chain, preserving data integrity and preventing duplication of personal data.
Consent and Ledger Layer	Clinical content is never kept on-chain; instead, consent state transitions and audit logs are recorded in a permissioned ledger. Smart contracts ensure GDPR and eIDAS compliance by managing the consent lifecycle (grant, update, suspend, revoke). This option promotes data minimisation and patient control over their information by guaranteeing that only authorised entities can alter consent data.
Interoperability Layer	Ensures compliance to the MyHealth@EU and EEHRxF standards for international health data exchange. Image data transfer is handled by DICOMweb, and metadata and consent management are handled by FHIR resources. Additionally, the layer facilitates conformance to these international standards, code system mappings, and localisation.

The Access and Authorisation Layer authorises patient actions against the live consent state after they are initiated in the Patient Interface Layer. While all actions are documented in the Consent and Ledger Layer, data operations (storage and retrieval) occur in the Data Storage Layer. Lastly, in accordance with FHIR and DICOMweb standards as well as European health frameworks such as EEHRxF and MyHealth@EU, the Interoperability Layer ensures that data remains transferable across national boundaries.

4.2.3. Trust and Security Features

This subsection defines the core mechanisms that protect confidentiality, integrity, availability, and accountability within the imaging wallet. Table 8 outlines the key features; Table 9 lists the minimal cryptographic and governance assumptions on which they rely.

Table 8 – Trust and Security Features.

Feature	Description
Decentralised Identity Management	A decentralised identity and related verifiable credentials are used to represent each actor, including patients and medical professionals. These approaches avoid reliance on a single central identity store, support high-assurance authentication across organisations and borders, and provide cryptographic proof of identity and attributes.
Smart Contracts for Consent Management	Smart contracts on a permissioned ledger include consent lifecycle logic. The contracts enforce scope, audience, and time-to-live parameters at decision time, regulate state transitions (grant, update, suspension, revocation), and bind access conditions to verified attributes. Revocation occurs as a result of subsequent authorisation checks and state changes.
Permissioned Ledger	Clinical content and comprehensive audit data are kept off-chain in a consortium ledger that records consent-state transitions and integrity anchors. Complete AuditEvent entries are stored in the FHIR store; only non-identifying commitments and policy states are recorded on-chain. Write and read permissions are limited to authorised health actors, ensuring accountability and tamper-evident provenance without duplicating personal information.

Table 9 – Minimal cryptographic and governance assumptions.

Area	Assumption
Key management	End-to-end encryption for imaging objects; patient keys generated client-side; provider keys issued by accredited institutions; private keys never on-chain; pragmatic rotation on credential change.
Revocation semantics	Revocation takes effect upon the ledger state change and the next authorisation check; propagation within the consortium is near-real-time.
Data minimisation	No clinical content or directly identifying personal data is stored on-chain; off-chain erasure deletes encrypted blobs and pointers; on-chain entries are limited to salted digests and policy states.
Ledger governance	Operated by accredited health actors under a published charter that sets out clear membership, change control, and audit rights; consensus is fault-tolerant within the consortium's quorum.

Tables 8 and 9 together form a logical control set. The permissioned ledger provides immutable consent and audit anchors while maintaining data minimisation by keeping clinical content off-chain; DID/VCs offer robust, portable identity; and smart-contract consent encodes a patient-centric authorisation model. These mechanisms implement the consent, ledger, identity, and governance decisions recorded in [ADR-01] [ADR-02] [ADR-03] [ADR-05] [ADR-08] [ADR-11].

4.2.3.1. Threat model and mitigations

Under the governance, token, and minimisation assumptions in [ADR-02] [ADR-03] [ADR-07] [ADR-11], the system operates in a permissioned consortium with sincere but inquisitive participants and a realistic endpoint compromise. The availability of the authorisation path, the confidentiality of imaging data, the integrity of consent and audit states, and the verifiability of decisions are protected assets. After verifying the live consent state, the access gateway issues a token, a temporary authorisation credential. Replay refers to the reuse of a previously valid artefact by a later or different host, such as a captured request or a copied bearer token.

Short-lived, audience-bound tokens with per-request nonces and, when supported, proof-of-possession binding to the caller's key reduce replay and token theft. The gateway compares every DICOMweb/FHIR request against the current consent state, ensuring that a recorded revocation instantly supersedes any captured artefact. The ledger never stores private keys, pixel data, or stable identifiers; all connections use mutual Transport Layer Security (TLS [63]) with eIDAS-recognised organisational certificates.

Pseudonym rotation, salted on-chain commitments, conservative deny-on-ambiguity behaviour, rate-limiting, and narrowly scoped emergency access with post-hoc review further reduce residual risks, including linkability, key compromise, validator misbehaviour, and abuse of emergency access. The DPIA sketch in Section 4.4.1 provides further detail on these elements.

4.2.3.2. Design-time service-level objectives

Instead of measuring guarantees, the PoC establishes indicative service-level objectives for the authorisation and audit path. These objectives provide guidelines for sizing, caching, and redundancy decisions, and set expectations for consent-check latency, revocation propagation, and the availability of the authorisation plane. These goals are treated as design-time assumptions related to [ADR-10] and form the foundation for NFR-04 (Availability & Reliability) and NFR-07 (Performance & Response Time). The corresponding Service Level Objectives (SLO [64]), their scope, and the supporting data at design time are shown in Table 10.

Table 10 – Design-time SLOs for the authorisation and audit path

Metric	Target	Scope and definition	Design-time evidence
Consent check latency (P95)	≤ 2 seconds	Time from the gateway receiving a protected request to issuing an allow or deny after consulting the live consent state	Architectural plane length, gateway caching strategy, single source of truth on the ledger
Revocation propagation bound	≤ 5 seconds	Time from ledger state change to enforced deny on all subsequent requests across the consortium	Short token lifetimes or introspection, quorum finality assumptions, deny-by-default on ambiguity
Authorisation plane availability	≥ 99.9% monthly	Uptime of the gateway, consent contract, and required trust services used to determine access	Redundancy and failover design, health checks and alerts, conservative degrade-to-deny behaviour

4.2.4. Cross-border Data Exchange

The constrained FHIR/DICOMweb surface described in Chapter 3 and [ADR-06] is essential for cross-border operation. While pixel data is always transferred via DICOMweb services (QIDO-RS/WADO-RS/STOW-RS), metadata about patients, providers, consent, and imaging studies is represented using profiled FHIR resources suitable for transport via MyHealth@EU national contact points. This separation of duties between FHIR and DICOMweb facilitates cross-border data exchange and compliance with EU legal and interoperability requirements, as shown in Table 11.

Under GDPR, eIDAS, and EEHRxF, these mechanisms combine DICOMweb retrieval of imaging objects with FHIR-based discovery and consent metadata. Each exchange generates append-only audit events while keeping clinical content off-chain, operationalising the interface profile anchors agreed in [ADR-06]. Revocation is enforced at retrieval time without re-issuing artefacts. Authorisation is based on verifiable credentials and consent artefacts.

Table 11 – Cross-border Data Exchange

Feature	Description
FHIR for Metadata	Consent artefacts, study and series descriptors, access events, and patient identity attributes use limited FHIR resources and profiles. This meets Myhealth@eu payload requirements and facilitates metadata discovery and exchange across jurisdictions.
DICOMweb for Imaging Data	Standardised DICOM retrieval and transfer via DICOMweb (QIDO-RS/WADO-RS/STOW-RS) ensures uniform management of studies and modalities across borders.
Compliance with EU Standards	Compliance with eIDAS for high-assurance identification and trust services, GDPR for lawfulness, purpose limitation, data minimisation, and auditability, and EEHRxF for MyHealth@EU's cross-border exchange patterns and document envelopes. Endpoint authentication and transport security use qualified certificates and EU trust lists.

4.2.5. Consortium governance

The ledger is managed by qualified authorities and accredited healthcare organisations that meet the requirements set out in a consortium charter. A supermajority is required to reach consensus on consent and revocation transactions, and validator nodes are distributed across jurisdictions to prevent single points of control. In line with governance decisions, membership changes, parameter updates, and operational incidents are formally documented and subject to independent audit, limiting single-jurisdiction dominance and providing EU-level verifiability. [ADR-02] [ADR-11].

4.3. Interoperability assumptions

The following outlines the minimal design-time assumptions required for the PoC to guarantee interoperability within a European context. By avoiding vendor-specific extensions or transport requirements, the focus is restricted to the datasets and operations that are absolutely required for imaging study viewing, consent management, and discovery. These assumptions reiterate the interface and data placement choices at the interoperability layer. [ADR-03] [ADR-04] [ADR-06] [ADR-12].

First, by focusing solely on patient-controlled discovery, consent, and viewing flows, the interoperability surface is deliberately limited. Reporting pipelines, workflow orchestration, and other ancillary uses are not included. Second, in line with widely accepted EU standards and to facilitate partner onboarding, all exchanges use DICOMweb for imaging payloads and FHIR for patient, provider, consent, and study metadata. Third, without implementing national connector specifics in this design-time proof of concept, cross-border operation conceptually complies with EEHRxF and MyHealth@EU expectations for payloads and trust.

Identity and trust assumptions demand high-assurance identities for clinical actors, verifiable credentials for roles, and qualified certificates for endpoints to ensure accountability in access decisions across different jurisdictions. Consent semantics are explicit and revocable,

designed to prevent artefacts from being reissued: details such as purpose, audience, and validity are specified in standard resources, enforced during access, and maintained across subsequent requests. Data placement assumes that imaging objects remain off-chain, with the ledger recording only non-identifying proofs and consent states to reduce data storage while ensuring auditability. Partners can handle access denials, identity failures, resource-not-found issues, and unsupported formats uniformly because error handling is predictable and machine-readable. Variations in national profiles are deferred to future work, as versioning and change control depend on stable descriptions of supported interactions and profile intent.

Interoperability is considered successful at design-time when the same patient-initiated share can be found and retrieved by different providers using only FHIR for metadata and DICOMweb for images. It is also successful when a revoked consent is enforced without re-issuing artefacts, and when access denial is presented in a way that any partner can understand and act upon, thanks to a consistent, machine-readable error.

4.4. Privacy and consent model

With a focus on privacy-preserving sharing across institutions and borders, this subsection outlines how patient consent is represented, enforced, and audited during the design phase. The consent statements and their operational implications are described in Table 12, which also indicates where enforcement occurs and what documentation is required for accountability.

Table 12 – Consent states and effects

State	Effect on access	Enforcement point	Audit expectation
Grant	Enables access within stated purpose, audience, scope, and validity interval.	Evaluated at request time against the current consent record.	Append a consent-grant event that captures the agreed parameters.
Update	Modifies purpose, audience, scope, or validity without interrupting care.	New parameters apply to subsequent requests immediately.	Append a consent-update event that describes the changed fields.
Suspend	Temporarily disables access without deleting artefacts or history.	Deny until suspension is lifted; no re-issuance required.	Append a suspension event with reason and, if set, duration.
Revoke	Terminates access; new requests are denied under the revoked grant.	Deny on the next authorisation check; prior disclosures unaffected.	Append a revocation event with a reason code.

To make the privacy posture explicit without repeating technical detail, Table 13 sets out the minimum guarantees and assumptions that govern data placement, purpose limitation, revocation behaviour, transparency, and cross-border applicability.

Table 13 – Privacy guarantees and assumptions

Area	Guarantee or assumption
Data placement and minimisation	No clinical content or personally identifiable data is recorded on-chain; only non-identifying proofs and consent/audit facts are recorded.
Consent scope and enforcement	Consent specifies the purpose, audience, scope, and validity; requests outside the scope are denied with a standard error at access time.
Revocation and emergency access	Revocation and suspension take effect with the next authorisation decision; time-critical break-glass is permitted for authenticated clinical roles, with reason capture and retrospective review.
Transparency and data subject rights	Every consent change and access decision generates an append-only audit event; the design supports access to records, rectification of metadata, and erasure of off-chain content and pointers.
Cross-border applicability	The same consent semantics and privacy guarantees apply uniformly across institutions and Member States engaged in the exchange.

Together, Tables 12 and 13 form a compact policy model in which consent is explicit, purpose-bound, and revocable; enforcement occurs at access time against the current state; auditability is thorough; and privacy is protected by stringent data minimisation and consistent behaviour across national boundaries. When combined, these regulations operationalise decisions about consent, minimisation, emergency access, and evidence bundles. [ADR-01] [ADR-03] [ADR-09] [ADR-13].

4.4.1. DPIA sketch and emergency access

The PoC covers patient-initiated imaging ingestion, encrypted off-chain storage of DICOM objects, creation and assessment of consent for sharing, authorisation of DICOMweb and FHIR requests from external providers, and the creation of audit and provenance records. Only non-identifying commitments and consent policy statements are recorded in the ledger, and special-category health data is encrypted and kept off-chain.

Explicit consent outlining the purpose, audience, scope, and validity is required for routine processing. Emergency access is based on vital interests, with rigorous scoping and retrospective review, when the patient is unable to give consent and urgent care is required.

Patients, healthcare providers, wallet and gateway operators, storage custodians, and consortium validators running a permissioned ledger are the only entities that can act as controllers or processors. No international transfers are required at this scope; storage and processing are limited to the European Economic Area (EEA), with mutual TLS and eIDAS-recognised certificates. Patient-facing controls for access, portability, and erasure via off-chain deletion and pointer or key rotation restrict retention to what is required for accountability. FHIR Consent, AuditEvent, and Provenance identifiers, as well as non-identifying ledger commitments with trusted time, serve as evidentiary anchors.

An overview of risk and mitigation., replay or reuse of authorisation artefacts, linkability and re-identification through metadata, key compromise on patient or provider devices, abuse of the emergency path, and invalidator behaviour are the primary risks. Examples of mitigations include audience-bound tokens with near-expiration dates, a one-time nonce per request with strict clock tolerance, optional proof-of-possession binding to the caller's key and required consent introspection at request time so that recorded revocation instantly overrides any captured artefact.

Rotating pseudonymous handles, per-object and per-state salted commitments, controlled-purpose codes instead of free text, bounded jitter in anchoring, uniform error semantics, and rate-limiting of high-frequency queries all reduce linkability. Attested server identities, separation and rotation of encryption and identity keys, out-of-band credential revocation, and hardware-backed key custody, when available, mitigate the risk of key compromise. Published validator eligibility, supermajority finality, on-chain change control, independent audit, and ongoing monitoring help reduce consortium risks. Correlating Consent, AuditEvent, and Provenance with the matching ledger commitment and, if applicable, a qualified timestamp ensures verifiability. These mitigations align with the technical and governance choices made in [ADR-03] [ADR-04] regarding tokens, minimisation, key custody, and consortium operation. [ADR-07] [ADR-10] [ADR-11] [ADR-12] [ADR-13].

In a emergency-access policy, the patient's inability to give consent and the presence of an urgent clinical need are triggering conditions. The data scope is restricted to the minimum required for the episode, and eligible actors are authenticated in their clinical roles at a defined assurance level. Tokens remain audience-bound, transient, and have a coded purpose; the authorisation path uses a vital-interests route in the gateway without changing the ledger consent state.

Every emergency use is logged with details of the actor, the reason, the scope, and the time. It automatically triggers an alert to oversight personnel, and any misuse can be reviewed afterwards for potential sanctions. Temporary artefacts are deleted after the episode ends, and regular consent-based controls resume, with the review's outcome documented. For thesis-level justification, this outline is sufficient; however, a full DPIA should be conducted with the relevant data protection officer before any deployment. The dedicated emergency-access decision [ADR-09] supports this approach.

4.5. User journeys

The PoC is demonstrated through four user journeys and the corresponding mock-ups. The summary is presented in Table 14. Each journey includes concise screen specifications after outlining the objective, main actor, entry requirements, and success criteria.

Table 14 – Overview of user journeys

Journey	Goal	Primary actor	Entry conditions	Success criteria
J1 – Patient upload	Add imaging studies to the wallet with correct metadata and default consent.	Patient	Patient is authenticated; imaging files available locally or via link.	Study stored off-chain; metadata indexed; integrity anchor created; default self-access consent recorded.
J2 – Cross-border share	Grant a foreign provider time-limited access to selected studies.	Patient and provider	Patient authenticated; provider presents high-assurance identity and role.	The provider can discover and retrieve only the consented studies within scope and validity.
J3 – Revocation	Withdraw an existing grant immediately.	Patient	An active consent grant exists.	Subsequent access attempts are denied and recorded in the audit, without re-issuing artefacts.
J4 – Audit inspection	Review who accessed what, when, and on what basis.	Patient (and auditor)	Audit trail exists.	Filtered timeline displayed; event details exportable; no clinical content exposed.

4.5.1. J1 – Patient upload

This journey illustrates how a patient ingests imaging into the wallet, using encrypted off-chain storage, non-identifying on-chain commitments, and a default self-access consent. It underpins RQ1 (deterministic authorisation from a single consent state) and RQ3 (data minimisation). The main patient-facing screens are sketched in APPENDIX D Figure 5-8.

The patient, authenticated with a DID and a high-assurance verifiable credential, opens the wallet, selects Upload, chooses one or more DICOM files or a study folder, and confirms, as shown in APPENDIX D, Figure 5. The wallet validates the input, encrypts the files client-side, and displays progress per item, as shown in APPENDIX D, Figure 6. Ciphertexts are sent to the off-chain storage service, which returns content locators. The wallet then computes salted digests of those locators and anchors an integrity commitment and a default self-access consent on the permissioned ledger as in APPENDIX D, Figure 7.

The journey ends with a confirmation that summarises the study and links to the audit entry, as shown in APPENDIX D, Figure 8.

If validation or encryption fails for a file, that item is skipped with a standards-compliant error, while the rest proceed. If the ledger is temporarily unavailable, the wallet queues the anchoring, marks the study as pending, and disables sharing until confirmation arrives. Persistent storage errors cause the affected item to be aborted but kept locally for later retry.

Technically, uploads may use DICOMweb STOW-RS, with metadata indexed via FHIR ImagingStudy or DocumentReference, and security events captured as FHIR AuditEvent and Provenance resources. The ledger records only salted digests, consent states and timestamps, never DICOM pixels, content identifiers, or directly identifying personal data, in line with [ADR-03] [ADR-04] [ADR-06] [ADR-08] [ADR-12]. A default self-access consent is anchored, with scope limited to the patient's own imaging and indefinite validity, unless later refined or revoked. Subsequent self-view or download operations are decided at request time from this live consent state, with short-lived, audience-bound tokens mediating access to FHIR/DICOMweb endpoints, as specified in [ADR-01] [ADR-07].

Security and privacy are enforced by client-side encryption, EU/EEA-resident off-chain storage, and wallet-held key pairs that are function-separated and rotated on lifecycle events, so that the compromise of a single key does not expose all content [ADR-03] [ADR-04] [ADR-12].

Design-time success for J1 is demonstrated when the off-chain repository contains an encrypted imaging study that is referenced by a corresponding FHIR ImagingStudy or DocumentReference resource, and a matching integrity commitment and consent state are anchored on the ledger. Together, the off-chain locator, the FHIR identifiers, and the ledger digest, transaction identifier, and AuditEvent reference constitute the minimal evidence bundle for a compliant upload and provide a verification path for [ADR-03] [ADR-04] [ADR-08].

4.5.2. J2 – Cross-border share

This journey illustrates how a patient grants a foreign healthcare provider time-limited access to selected imaging studies, constrained by scope and purpose, and how retrieval is then deterministically authorised via DICOMweb/FHIR. It supports RQ1 (deterministic authorisation from a single consent state) and RQ3 (data minimisation), and exercises the cross-border, consent and token decisions in [ADR-01] [ADR-02] [ADR-05] [ADR-06] [ADR-07]. The patient-facing steps are illustrated in APPENDIX D, Figure 9-12.

The patient is authenticated at high assurance using a DID and a verifiable credential. The relying party is a foreign provider whose organisational identity and role attributes are presented via an eIDAS-aligned assertion. The permissioned ledger, access gateway and interoperability endpoints are reachable. At least one study is already present in the wallet, with completed integrity and consent anchoring, and the intended provider can be resolved to a trusted organisational identity.

From the Share screen, the patient selects one or more studies and the target provider, as shown in APPENDIX D, Figure 9. The wallet displays the provider's verified identity and role and prompts the patient to confirm the purpose of use, scope, and validity window, as shown in APPENDIX D, Figure 10. On confirmation, a consent grant is recorded to the ledger, constrained by scope, audience, purpose code, and validity; finality is confirmed, and the access gateway derives a short-lived, audience-bound token template reflecting those parameters, as shown in APPENDIX D, Figure 11. A standards-conformant share link or referral is prepared, and the patient sees a summary with options to copy or hand off via the national contact point and to revoke control immediately, as shown in APPENDIX D, Figure 12. When the provider later calls DICOMweb/FHIR, the gateway checks the live consent state and issues or validates scoped tokens only if all conditions are met; all retrieval attempts are logged.

If the provider's identity cannot be verified to the required assurance level, the wallet refuses to proceed and suggests alternative verification. If the patient restricts the scope to a study that is later removed, discovery yields a standards-conformant not-found, and the share becomes inert. If the ledger is temporarily unavailable, the consent grant is queued, the share is marked pending, and no live link is exposed until anchoring succeeds. Any out-of-scope request that is expired or mis-audited results in a deterministic deny, a clear machine-readable error, and an FHIR AuditEvent with outcome deny.

The journey covers FHIR Consent for the grant, ImagingStudy and/or DocumentReference for scoped studies, and AuditEvent and Provenance for recording the issuance and use of tokens. At the foreign provider, DICOMweb QIDO-RS and WADO-RS are used to query and retrieve only those studies covered by the consent, based on pseudonymous identifiers carried in tokens. The ledger records only salted commitments and consent state transitions, keeping policy state and clinical content strictly separate in line with [ADR-03] [ADR-04] [ADR-06] [ADR-08].

Consent is expressed through an explicit purpose code, a limited audience to the selected provider, a defined validity interval, and scope over the chosen studies or series. The gateway derives short-lived, audience-bound tokens from this state; each token carries claims for scope, purpose and expiry, which are enforced on every request. Any mismatch in subject, scope, audience, purpose or time results in a deny outcome, implementing request-time consent evaluation and token semantics as in [ADR-01] [ADR-07].

From a security and privacy perspective, the wallet never directly exposes pixel data. It only surfaces pseudonymous references and scoped tokens; pixels and identifiers remain off-chain and encrypted, and decryption keys remain within the patient-centred key store. Token

misuse is limited by short lifetimes, audience binding and continuous logging, consistent with [ADR-03] [ADR-04] [ADR-07] [ADR-12].

Design-time success for J2 is demonstrated when the ledger contains a consent-grant transaction with the expected purpose, audience and validity; the gateway can issue and validate scoped tokens that allow in-scope retrievals and deny out-of-scope or expired requests; and FHIR AuditEvent records exist for both successful and rejected calls. Together, these artefacts form the minimal evidence bundle for cross-border sharing and provide a verification path for [ADR-01] [ADR-02] [ADR-06] [ADR-08] [ADR-13].

4.5.3. J3 – Revocation

This journey illustrates how a patient withdraws previously granted consent and how subsequent DICOMweb/FHIR requests are deterministically denied without reissuing artefacts, in accordance with the defined revocation semantics. It primarily supports RQ2 (effective, provable revocation tied to a time reference) and reinforces RQ1 (single source of truth for allow/deny decisions). The patient-facing entry point for managing existing shares is illustrated in APPENDIX D, Figures 13-16.

The patient is authenticated at high assurance using a DID and a verifiable credential. The permissioned ledger and access gateway are reachable, and at least one foreign provider holds an active grant created in J2 and uses the gateway to retrieve it. A corresponding FHIR Consent resource exists with an active state, scope, audience, and validity, and the wallet can access the consent contract and audit service. Connectivity to the FHIR store and DICOMweb endpoint is available, though no pixel transfer is required for the revocation itself.

From the Shares view, the patient selects an active grant, as shown in APPENDIX D, Figure 13. The wallet displays the provider identity, purpose code, scope and validity, along with a Revoke action and a brief explanation of the consequences. When the patient chooses Revoke, they confirm and, optionally, select a reason code, as shown in APPENDIX D, Figure 14. The wallet submits a consent state transition to revoked on the ledger and waits for finality; during this step, progress and, where available, a qualified timestamp reference are shown, as in APPENDIX D, Figure 15. Once confirmed, the gateway consults the updated consent state at request time and denies any subsequent provider call based on that grant. The flow ends with a summary screen linking to the revocation audit entry and noting that further requests are denied and logged, as in APPENDIX D, Figure 16.

If the ledger cannot be reached, the wallet records the intent locally, marks the grant as revocation pending, and blocks further sharing actions tied to that grant. While the state is ambiguous, the gateway follows a conservative deny-on-doubt policy. If the patient chooses to suspend rather than revoke, a temporary state is applied that denies requests until suspension is lifted. If the provider issues requests during the short window between submission and finality, the gateway evaluates the transaction horizon and consent state such that, where policy requires, requests in that window are also denied and logged, avoiding race conditions.

At the standards level, the FHIR Consent resource is updated to status revoked, and a state transition on the ledger mirrors this change. A FHIR AuditEvent records the revocation, and any post-revocation attempts generate AuditEvent entries with outcome deny and, where relevant, a standards-conformant OperationOutcome explaining the error. No DICOMweb pixels are transferred during this journey; later WADO-RS requests based on the revoked consent are deterministically denied, reflecting the revocation, minimisation and evidence decisions in [ADR-01] [ADR-03] [ADR-08] [ADR-13].

Revocation is implemented as a state change anchored on the ledger and reflected in the wallet's consent view. The access gateway evaluates each request against the live consent state, using introspection or short-lived, audience-bound tokens so that no previously issued artefact can override the updated state. Any mismatch in state, scope, audience, purpose or time results in an immediate deny decision, in line with the token and revocation semantics in [ADR-01] [ADR-02] [ADR-10].

Only non-identifying facts are recorded on-chain: a salted commitment to the revoked-consent state, its timestamp, and the identifier of the revoking actor. Encrypted image content and its locators remain off-chain and encrypted end-to-end; decryption keys are never disclosed after revocation and attempts to reuse old tokens are rejected in accordance with the propagation and caching strategies in [ADR-01] [ADR-02] [ADR-10] [ADR-12] [ADR-13].

Design-time success for J3 is demonstrated when the ledger reflects a revocation state with an anchored time reference; subsequent access attempts via the revoked grant or its tokens are denied within the assumed propagation bound; and FHIR AuditEvent entries document both the revocation action and the denied requests. Together, these artefacts provide the verification hook for the revocation semantics and quality assumptions referenced in [ADR-01], [ADR-02], and [ADR-10].

4.5.4. J4 – Audit inspection

This journey demonstrates how a patient or authorised auditor can reconstruct an end-to-end access episode without exposing pixel data, using only standard FHIR artefacts linked to on-chain anchors. It primarily supports RQ4 (auditability and evidence bundle) and contributes to RQ2 by enabling post hoc verification of revocation effects. The entry surface for selecting the study and time window is illustrated in APPENDIX D, Figures 17-20.

The main actors are the patient and, optionally, an auditor with read-only observer rights; both authenticate at high assurance. The FHIR store, permissioned ledger and audit viewer are reachable, and the wallet holds a keypair to request a signed export when needed. At least one study has prior activity (upload, share, retrieval or revocation), with corresponding FHIR Consent and AuditEvent entries and a non-identifying consent-state anchor on the ledger.

In the Audit section, the user selects a study and a time window and views a timeline with filters for actor, outcome and purpose, as in APPENDIX D, Figure 17. Selecting an event opens a detail panel that shows the actor, action, and outcome, along with links to the related Consent and Provenance resources, as in APPENDIX D, Figure 18. Tapping Reconstruct episode prompts the wallet to query the FHIR store for all AuditEvent and Provenance items linked to the study, correlate them with the consent state anchored on the ledger for the relevant period, and display progress, as in APPENDIX D, Figure 19. The result is a consolidated narrative and a minimal evidence bundle that can be exported and digitally signed, as in APPENDIX D, Figure 20.

If some partners do not emit AuditEvent entries for specific actions, the viewer marks the reconstruction as partial, explicitly indicating gaps while preserving available entries. If the ledger is temporarily unreachable, reconstruction proceeds solely from FHIR, and the on-chain corroboration is flagged as pending. When an auditor is the user, the interface redacts patient-identifying User Interfaces (UI) elements and shows only pseudonymous handles and coded attributes, preserving minimisation.

The journey uses FHIR AuditEvent for decisions and outcomes, FHIR Consent for the authorising policy at the time, and FHIR Provenance (where present) to link events to specific actors or systems. It may dereference ImagingStudy or DocumentReference metadata for non-identifying study details but never retrieves pixel data. The ledger is consulted only to verify the corresponding salted consent-state anchor, corroborating that the off-chain FHIR records are consistent with an immutable, non-identifying commitment, in line with [ADR-03] [ADR-08] [ADR-13].

Reconstruction is strictly read-only: it grants no new access. It simply interprets past decisions recorded in AuditEvent, considering the consent state that applied at the time, as encoded in FHIR Consent and anchored on the ledger. For each event, the tool checks whether the observed outcome (permit or deny) matches the then-current consent parameters; discrepancies are highlighted as potential violations of the deterministic decision model, reusing the same consent semantics as live authorisation in [ADR-01] [ADR-03].

No clinical content is exported. The evidence bundle contains only pseudonymous correlation handles, coded scope and purpose, timestamps, decisions, and consent-state anchors; it excludes pixel data and directly identifying personal health data, in line with the minimisation posture in [ADR-03] [ADR-08] [ADR-13].

Design-time success for J4 is achieved when the user can produce a coherent, time-ordered narrative of who accessed which imaging studies, for what declared purpose, under which consent, with what outcome, and when that narrative can be corroborated against the on-chain consent-state anchor. This provides the primary verification path for RQ4 and for the evidence-bundle decisions captured in [ADR-08] and [ADR-13].

4.6. Evaluation approach at design-time

This chapter's method analyses the architecture by examining the behaviour of four journeys and associated evidence bundles. It relies on European standards rather than direct measurements. The journeys, architectural touchpoints, and evidence artefacts expected to demonstrate conformance or identify violations are aligned with each research question (RQ1–RQ4), as shown in Table 15. To connect the success or failure of each research question to specific decisions [ADR-01–ADR-13], the architectural locus column also references relevant ADRs in Section 3.3.1, where applicable. Sections 4.7 and 4.8 discuss the specific limitations of this analytical approach.

Table 15 – Research question alignment and evidence.

RQ	Claim to be shown	Architectural touchpoints	User journey	Evaluation method	Evidence artefacts
RQ1	Authorisation decisions for DICOMweb/FHIR are deterministic from a single consent state.	Ledger consent state (anchor/contract); access gateway enforcement	J1, J2	Reason about a single source of truth consulted at request time.	Allow or deny outcome based on consent state; scoped token claims; AuditEvent outcome entries.
RQ2	Revocation prevents valid access after time T and is provable.	Consent state transition and time reference; gateway deny path	J3	Show state change to revoked and the absence of successful access after T.	On-chain revocation transaction id; qualified timestamp if used; deny AuditEvent entries post-T.

RQ	Claim to be shown	Architectural touchpoints	User journey	Evaluation method	Evidence artefacts
RQ3	On-chain records are non-identifying and do not disclose personal health data.	Data-placement policy; on-chain commitment schema (hashing/salting strategy)	J1–J4	Inspect recorded fields and prove the absence of personal data concerning health and stable identifiers.	Salted commitment values and policy statements only; no pixel data; no stable identifiers.
RQ4	An access episode can be reconstructed end-to-end using standard resources.	FHIR AuditEvent, Provenance and Consent; linkage to ledger consent-state anchors	J4	Correlate timeline entries and policy state at decision times.	Linked resource identifiers; signed evidence bundle; reference to consent-state anchor.

A more detailed FR/NFR traceability view is given in Table 17 and Table 18 in Appendix A, an expanded definition of the evidence bundle is presented in Appendix A Table 19.

4.7. Findings and open issues

The design-time evaluation supports four key findings:

- Deterministic authorisation. When every DICOMweb/FHIR request is mediated by the access gateway and decided from a single consent state anchored on the permissioned ledger, the allow/deny outcomes in J1-J3 follow directly from that invariant.
- Effective revocation. Revocation operates as a consent-state transition: once the change is recorded on the ledger, subsequent requests are denied without reissuing artefacts. They can be tied to a trusted time reference.
- Ledger minimisation. Across all journeys, clinical pixels and stable identifiers remain off-chain; on-chain entries are limited to salted commitments and policy states, preventing the ledger from becoming a secondary health-data repository.
- End-to-end auditability. J4 shows that by correlating FHIR Consent, Provenance and AuditEvent, an access episode can be reconstructed in a way that is intelligible to patients and verifiable by oversight bodies, without exposing protected content.

Nonetheless, several promising but unproven aspects remain. Although unmeasured, the service-level goals for consent verification and revocation propagation are architecturally plausible at design time. Their achievement depends on the latency of external trust services, the cache strategy, and the deployment topology. In theory, cross-border operations are consistent with EEHRxF and MyHealth@EU, but in practice, connector behaviour, code systems, and error semantics may vary. Although identity assurance based on DIDs and eIDAS-aligned credentials appears sufficient, operational integration with the EUDI Wallet and healthcare credential ecosystems remains outside the scope of the present evaluation.

Additionally, all participants must emit standard-compliant AuditEvent entries for the audit to be complete, which may not always be the case across diverse clinical infrastructures.

Real-world testing and governance rehearsal are the only ways to solve some problems. To ensure that consortium governance offers both safety and liveness under realistic fault conditions, such as node compromise and network partition, validator eligibility, quorum design, and incident response require empirical testing. Operational patterns that maintain sovereignty without introducing new single points of failure need to be addressed for key custody and patient recovery (device loss, guardianship, minors, deceased users). Organisational safeguards and post-hoc review capabilities are essential to maintain break-glass's limited scope and auditable nature. Monitoring and, if required, more robust pseudonym rotation and rate-limiting than those assumed at design time are needed to mitigate linkability risks arising from timing or usage patterns. Long-term cryptographic agility, including potential post-quantum migration, needs to be considered to prevent lock-in of commitments and signatures. Interoperability edge cases, such as series-level consent, mixed-modality studies, and legacy PACS behaviour, should be tested in partner testbeds.

When considered collectively, these results show that the PoC is defensible at design time for the claims of determinism, revocation, minimisation, and auditability, while identifying a limited number of unresolved issues related to deployment, governance, and empirical performance. These boundaries are clarified, and the underlying presumptions of the current evaluation are identified in the following section on limitations and validity.

4.8. Limitations and validity

This chapter's evaluation is analytical and design-time. Rather than running a system, it makes the case for correct authorisation, revocation, minimisation, and auditability by analysing journey-level artefacts and reasoning about architectural responsibilities. Therefore, rather than empirical performance, operational robustness, or usability in real clinical settings, the conclusions relate to the conceptual model and its alignment with standards.

4.8.1. Scope and methodological boundaries

Usability testing, fault-tolerance testing, and runtime benchmarking were not conducted. Consent verification and the revocation propagation service are design objectives rather than quantifiable results. Mock-ups show expected interactions, but they don't replace workflow validation with clinicians or accessibility testing with a variety of patient populations. Although

data placement and the use of qualified trust services are used to argue for security properties such as confidentiality, integrity, and non-repudiation, these properties ultimately depend on proper cryptographic implementation, key custody, and secure coding - all of which are outside the purview of this thesis.

4.8.2. Assumptions underpinning the claims

The argument for privacy and determinism rests on explicit assumptions. The ledger achieves timely finality under a supermajority quorum, is permissioned, and is overseen by recognised health actors. DIDs and eIDAS-aligned credentials provide high-assurance identity for both patients and providers. When evidentiary anchoring is needed, qualified timestamp services can be contacted. Off-chain storage enforces encryption both in transit and at rest while remaining within EU/EEA jurisdictions. To prevent stale authorisations, the access gateway compares requests to live consent states or short-lived tokens. Participating systems consistently emit standard-conformant AuditEvent entries. Patient devices have secure key material, and protocols are in place for recovering lost or replaced keys. The strength of the corresponding claim is diminished if any of these assumptions is compromised.

4.8.3. Threats to validity and generalisability

Mapping research questions to journeys and evidence artefacts supports construct validity, but edge cases such as series-level consent, mixed-modality studies, or different scope encodings may require additional artefacts and a more detailed evaluation. Internal validity can be affected by delays and concurrent events around revocation; enforcement relies on tightly bound token lifetimes and real-time consent checks to ensure deny outcomes after revocation. External validity faces jurisdictional variability; standards-compliant implementations may still need local adjustments due to differences in National Contact Point for eHealth (NCPeH) connectors, national codes, and error handling. Legacy PACS/VNA integration can reveal constraints like non-uniform DICOM compliance and data quality issues. Privacy can be compromised by timing and usage patterns; without pseudonym rotation and rate-limited access, linkability can occur even with non-identifying on-chain entries.

4.8.4. Ethical and legal considerations

This data-protection impact analysis is not a complete DPIA but a sketch. While governance mechanisms for post-hoc review, redress, and supervisory oversight rely on organisational

capacity beyond technical design, routine processing is based on explicit consent and emergency access in critical interests. In terms of guardianship, delegation, and post-mortem record handling, special populations (minors, incapacitated patients, deceased users) add extra complexity. By design, rights such as erasure and portability are implemented through off-chain deletion and on-chain state changes involving pointer or key rotation, leaving residual audit anchors. This structural conflict between minimisation and accountability needs to be resolved transparently and legally. Lastly, during deployment, interpretations of EHDS, EEHRxF, and the EUDI framework may change as standards and regulations evolve.

4.8.5. Implications for future evaluation

Each research question is summarised in Table 16, along with how it is addressed in the current design-time evaluation and what a corresponding empirical track would entail once testbeds and prototypes are available.

Table 16 – Research questions: current evaluation and future empirical work

Research question	Addressed in this thesis (design-time evaluation)	Future empirical evaluation
RQ1. Are authorisation decisions for DICOMweb/FHIR requests deterministic when derived from a single live consent state?	All DICOMweb/FHIR requests are mediated by the access gateway and determined by a single current consent state on the ledger, with deny-by-default behaviour in cases of ambiguity, according to an analytical evaluation of the architecture, design invariants, and journeys J1–J2 (see Table 15).	Deploy a prototype wallet, gateway, and ledger; execute scripted imaging workflows across providers; and confirm that audit logs and observed allow/deny outcomes consistently match the then-current consent state, including under load, failures, and race conditions.
RQ2. Does revocation prevent valid access after a given time T in a way that can be evidenced and verified?	Modelled as a state transition on the ledger, with a bounded propagation window enforced by the gateway and recorded in journey J3: logs and evidence show that no legitimate access path remains after time T without new consent artefacts.	Revoke consent while clients have active tokens to implement revocation and measure propagation in an operational system. Track how long it takes for all subsequent requests to be rejected, and evaluate whether operators and auditors can understand this behaviour based on the generated evidence.
RQ3. Do on-chain records remain non-identifying, avoiding the storage of personal data concerning health or stable identifiers?	As demonstrated in journeys J1–J4, the proposed data-placement policy and on-chain schema address this issue by placing only salted commitments and policy states on the ledger, leaving pixels and directly identifying attributes off-chain, encrypted.	Examine complete ledger snapshots and conduct re-identification solely from on-chain entries to support privacy and data-protection reviews of concrete deployments. This includes adversarial linkage analyses and stress tests of the salting and pseudonym-rotation strategy.
RQ4. Can an access episode be reconstructed end-to-end using standard resources (e.g., FHIR Consent, AuditEvent and Provenance) combined with non-identifying ledger anchors?	Conceptually assessed in journey J4 and the minimal evidence bundle: without retrieving pixel data, an access episode is reconstructed from FHIR Consent, AuditEvent, and Provenance, correlated with non-identifying ledger anchors.	Create an audit and evidence viewer using this reconstruction, and conduct task-based studies with auditors, patients, and clinicians to assess their ability to understand access histories, identify irregularities, and trust the evidence provided in practical situations.

The summary in Table 16 clearly states that, rather than relying on runtime measurements or user studies, the current work addresses RQ1–RQ4 at design time through architectural reasoning, user journeys, and the inspection of standards-based artefacts. Sections 4.8.1 to 4.8.4 provide details on the scope, underlying assumptions, and potential threats to the validity of this analytical approach.

These limitations directly inform future empirical research. It is essential to measure the propagation of consent verification and revocation under realistic topologies and loads. National profiles and code systems should be used in partner testbeds to practise cross-border interoperability. To verify safety and liveness, consortium governance should be exercised through fault injection and incident simulations. Structured research involving patients and clinicians is necessary for usability and accessibility. Cryptographic-agility plans should be prepared for future algorithmic migrations, and privacy should be stress-tested through adversarial analyses of linkability and side channels. Chapter 5 discusses these activities as future work, extending the present design-time argument into operational assurance without altering the fundamental architectural commitments established in this chapter.

CHAPTER 5

Discussion and Conclusions

5.1. Discussion

5.1.1. Restating objectives and research questions

In line with European regulations and interoperability frameworks, this thesis aimed to design and assess, during the design phase, a patient-centric imaging wallet that integrates a permissioned ledger, decentralised identity, and off-chain encrypted storage. The four research questions (RQ1–RQ4) that guided the work were the determinism of authorisation, the effectiveness of revocation, strict on-chain data minimisation, and the ability to reconstruct access episodes end-to-end using standard artefacts. Chapters 3 and 4 addressed these issues through a conceptual architecture, ADRs [ADR-01–ADR-13], and a PoC presented through user journeys.

5.1.2. Synthesis of findings against RQ1-RQ4

The findings support affirmative responses to all four questions at design time. Enforcing a single authorisation plane, in which each DICOMweb/FHIR request is determined by a single live consent state mediated by the access gateway, addresses RQ1. Modelling revocation as a ledger state transition with a bounded propagation window, after which no successful access is possible without re-issuing artefacts, satisfies RQ2. Strict data placement satisfies RQ3: pixels and detailed audits remain off-chain under encryption, while only salted commitments and policy states appear on-chain. FHIR Consent, AuditEvent, and Provenance, together with ledger anchors, support RQ4 by enabling access to episode reconstruction without disclosing clinical content.

5.1.3. Alignment with European standards and policy initiatives

GDPR, eIDAS, EEHRxF, MyHealth@EU, and the developing EHDS have all influenced the architecture. Explicit, revocable consent, privacy by design through off-chain encrypted storage, and data minimisation on the ledger are examples of how GDPR principles are reflected. DIDs and verifiable credentials at high assurance for patients and providers are anticipated for eIDAS and the upcoming EUDI Wallet. Regarding interoperability, the imaging wallet is positioned as a supplementary, patient-facing element rather than a substitute for

national infrastructures or NCPeH connectors, given its reliance on DICOM/DICOMweb and HL7 FHIR, both of which are limited by EU profiles.

5.1.4. Positioning relative to related work and real cases

A large portion of the blockchain-for-health literature focuses on areas such as supply chains and clinical trials rather than imaging, or it centres on public chains, tokenisation, or broad data replication, which conflicts with GDPR minimisation and erasure [65]. A patient-controlled imaging wallet is not yet available, and real EU initiatives such as MyHealth@EU cross-border exchanges usually use FHIR/IHE profiles without blockchain [40], [66]. This thesis sits between these strands by proposing a consortium-governed, permissioned ledger that is specifically aligned with EU standards, tightly integrated with DICOMweb and FHIR, and used only for non-identifying commitments and consent states. In doing so, it provides a conceptual framework that can guide future pilots seeking to integrate cross-border interoperability, verifiable consent, and patient control.

5.1.5. Implications for practice and research

The thesis proposes that, if blockchain integration remains within existing PACS/VNA and NCPeH infrastructures and its function is limited to anchoring consent and provenance, it can be utilised in imaging without creating a separate health data repository. The minimal evidence bundle and single authorisation layer can serve as helpful checklists for evaluating other proposals. In cases of limited implementation resources, the study underscores the importance of treating research questions as design invariants and relying on a standards-based, design-time evaluation. It also stresses the need for interdisciplinary collaboration, given that key decisions, such as identity assurance, consent semantics, and governance, are situated at the crossroads of distributed systems and European digital policy.

5.2. Future Work

5.2.1. Technical implementation and performance evaluation

Implementing a minimal working prototype of the imaging wallet, access gateway, ledger, and off-chain services, ideally integrated with a test PACS/VNA, is a logical next step. This would test the design-time service-level objectives and identify functional bottlenecks or configuration constraints by enabling empirical measurement of consent-check latency, revocation propagation, throughput, and fault tolerance under realistic conditions.

5.2.2. Usability, accessibility and clinical integration

Future research should also focus on accessibility and usability by conducting systematic assessments with physicians and patients. Users' understanding of consent options, revocation and sharing flows, and whether the extra steps fit into actual clinical workflows can be evaluated by prototyping the wallet interface and conducting task-based studies. To prevent exacerbating existing disparities in access to digital health tools, special consideration should be given to multilingual support, accessibility guidelines, and populations with lower levels of digital literacy.

5.2.3. Governance, legal and ethical consolidation

Legal consolidation and practical rehearsal are necessary for the governance model described in this thesis. Governance playbooks for validator admission, incident response, key compromise, and dispute resolution, including fault-injection exercises to test safety and liveness under challenging circumstances, need to be developed. Before deployment, a thorough DPIA and engagement with ethics committees, supervisory authorities, and patient organisations would be necessary, particularly regarding minors, delegation, deceased patients, and the alignment of rights such as erasure and portability with accountability (audit anchors).

5.2.4. Generalisation beyond imaging and long-term evolution

Lastly, the method could be investigated over longer time horizons and beyond imaging. If suitable FHIR profiles are available, the wallet and consent model could be adapted to other types of health data to test the design's scalability across domains. To prevent even non-identifying on-chain entries from becoming a source of re-identification at scale, future research should investigate migration paths to post-quantum primitives and stress-test metadata and usage patterns. Long-term evolution also raises concerns about cryptographic agility and resistance to linkability.

5.3. Concluding remarks

This thesis began with a specific issue: while regulatory initiatives such as the GDPR, eIDAS, and the developing EHDS demand stronger guarantees of consent, accountability, and data minimisation, medical imaging in Europe remains fragmented across institutional and national silos. As demonstrated in Chapter 2, there is currently no patient-controlled, imaging-specific wallet design that is explicitly aligned with EIFs and treats consent, revocation, and auditability

as first-class design concerns rather than afterthoughts, despite the growing body of work on blockchain in healthcare and EHR exchange.

A conceptual architecture for a patient imaging wallet that incorporates a permissioned ledger, decentralised identity, and off-chain encrypted storage, anchored in established profiles for DICOMweb, HL7 FHIR, the EEHRxF, and MyHealth@EU, has been proposed to address this gap. Rather than treating the ledger as an add-on to institutional portals, this architecture places the patient wallet and the access gateway at the centre of imaging flows, extending previous proposals. As a result, it addresses the deficiency in wallet-centric, imaging-oriented designs in the European context highlighted by the literature review.

A set of design invariants that enforce deterministic authorisation from a single consent state, effective and provable revocation, strict on-chain data minimisation, and end-to-end auditability was then developed in response to the research questions. The work addresses earlier research that primarily discusses consent management, privacy, and interoperability in qualitative terms without outlining how these guarantees constrain interfaces and data placement, treating these properties as invariants that must hold across wallet, gateway, ledger, and storage. Under European regulation, the invariants specify what must be true of any implementation that purports to meet the requirements of a patient-centric imaging wallet.

Lastly, the thesis presents a design-time proof of concept that links architectural elements to DICOM and FHIR artefacts, as well as to GDPR and eIDAS obligations. This proof of concept is expressed through user journeys, evidence bundles, and traceability matrices. By demonstrating how a blockchain-enabled architecture can be evaluated for conceptual viability, compliance alignment, and interoperability using standards-based artefacts alone, this addresses the lack of structured evaluation approaches in the state of the art. It also makes clear the boundaries of this work: once tangible implementations are available, performance, usability, security testing, and long-term governance still need to be empirically investigated.

Collectively, these contributions suggest that a patient imaging wallet, built on explicit invariants and European interoperability standards, can provide a logical way to improve patient control and enable cross-border, verifiable sharing of imaging data without placing clinical content on the chain. They also outline a clear agenda for upcoming organisational experiments, technical pilots, and policy discussions on the governance and adoption of such wallets in real-world healthcare systems.

Bibliographic References

[1] 'European Health Data Space Regulation (EHDS) - European Commission'. Accessed: July 20, 2025. [Online]. Available: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en

[2] J. Karacic Zanetti and R. Nunes, 'To Wallet or Not to Wallet: The Debate over Digital Health Information Storage', *Computers*, vol. 12, no. 6, p. 114, May 2023, doi: 10.3390/computers12060114.

[3] 'Impact Assessment on the European Health Data Space - European Commission'. Accessed: July 20, 2025. [Online]. Available: https://health.ec.europa.eu/publications/impact-assessment-european-health-data-space_en

[4] European Commission, 'The New European Interoperability Framework', ISA^2 - European Commission. Accessed: July 20, 2025. [Online]. Available: https://ec.europa.eu/isa2/eif_en/

[5] 'Regulation - 2016/679 - EN - gdpr - EUR-Lex'. Accessed: July 20, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[6] A. Anderberg *et al.*, 'Blockchain Now And Tomorrow', JRC Publications Repository. Accessed: July 20, 2025. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/handle/JRC117255

[7] A. Ali *et al.*, 'Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain', *Electronics*, vol. 10, no. 16, p. 2034, Aug. 2021, doi: 10.3390/electronics10162034.

[8] 'Decentralized Identifiers (DIDs) v1.0'. Accessed: July 20, 2025. [Online]. Available: https://www.w3.org/TR/did-1.0/

[9] D. T. Harrell *et al.*, 'Technical Design and Development of a Self-Sovereign Identity Management Platform for Patient-Centric Healthcare Using Blockchain Technology', *Blockchain Healthc. Today*, Mar. 2022, doi: 10.30953/bhty.v5.196.

[10] 'European Digital Identity - European Commission'. Accessed: July 20, 2025. [Online]. Available: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

[11] 'IPFS: Building blocks for a better web', IPFS. Accessed: July 20, 2025. [Online]. Available: https://ipfs.tech

[12] OECD, *Health in the 21st Century: Putting Data to Work for Stronger Health Systems*. in OECD Health Policy Studies. OECD, 2019. doi: 10.1787/e3b23f8e-en.

[13] M. Eichelberg, K. Kleber, and M. Kämmerer, 'Cybersecurity in PACS and Medical Imaging: an Overview', *J. Digit. Imaging*, vol. 33, no. 6, pp. 1527–1542, Dec. 2020, doi: 10.1007/s10278-020-00393-3.

[14] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*. 2021. Accessed: Dec. 21, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[15] 'EHRxF Electronic Health Record exchange Format |'. Accessed: July 20, 2025. [Online]. Available: https://ehr-exchange-format.eu/

[16] 'EU Digital Identity Wallet Home - EU Digital Identity Wallet -'. Accessed: July 20, 2025. [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home

[17] D. Conway, M. Venkataraman, D. Laverick, G. Pelin, and A. Hasselgren, 'Blockchain in Healthcare Today 2022 Predictions', *Blockchain Healthc. Today*, Jan. 2022, doi: 10.30953/bhty.v5.194.

[18] 'Index - FHIR v5.0.0'. Accessed: July 20, 2025. [Online]. Available: https://hl7.org/fhir/

[19] 'DICOM', DICOM. Accessed: July 20, 2025. [Online]. Available: https://www.dicomstandard.org

[20] Elsevier, ‘Scopus - Document search’, Elsevier. Accessed: June 02, 2025. [Online]. Available: https://www.scopus.com/search/form.uri?display=basic#basic
[21] IEEE, ‘IEEE Xplore Digital Library’, Institute of Electrical and Electronics Engineers. Accessed: June 02, 2025. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp
[22] ‘Document Search - Web of Science Core Collection’. Accessed: July 20, 2025. [Online]. Available: https://www.webofscience.com/wos/woscc/basic-search
[23] M. J. Page *et al.*, ‘The PRISMA 2020 statement: an updated guideline for reporting systematic reviews’, *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.
[24] S. M. Shah and R. A. Khan, ‘Secondary Use of Electronic Health Record: Opportunities and Challenges’, *IEEE Access*, vol. 8, pp. 136947–136965, 2020, doi: 10.1109/access.2020.3011099.
[25] V. S. Moorthy, K. Saravanan, H. B, S. Saravanan, and R. G. J, ‘Verified Access to EHR over Blockchain and IPFS with Lit Protocol Encryption’, in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, Pune, India: IEEE, Oct. 2024, pp. 1–7. doi: 10.1109/icbds61829.2024.10837546.
[26] L. R. Peddu, A. Mishra, A. R. L. Padmaja, R. G, P. S, and R. K. Pongiannan, ‘MediVault DApp: A Electronic Health Record Application Using Blockchain Technology’, in *2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, Prawet, Thailand: IEEE, Mar. 2025, pp. 1914–1919. doi: 10.1109/icmlas64557.2025.10967615.
[27] F. Hasan, D. Dakhane, and A. Vidhate, ‘AES Encryption for Secure Storage and Transfer of Patient Health Records using Blockchain Technology’, in *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India: IEEE, Nov. 2023, pp. 568–575. doi: 10.1109/icccis60361.2023.10425583.
[28] C. Lu, Z. Yu, G. Wang, A. Dong, and X. Tian, ‘A Blockchain-based PHR Sharing Scheme with Attribute Privacy Protection’, in *2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Sanya, China: IEEE, Dec. 2024, pp. 2068–2077. doi: 10.1109/trustcom63139.2024.00287.
[29] L. Sun, D. Liu, Y. Li, and D. Zhou, ‘A Blockchain-Based E-Healthcare System With Provenance Awareness’, *IEEE Access*, vol. 12, pp. 110098–110112, 2024, doi: 10.1109/access.2024.3440170.
[30] S. Abbate, P. Centobelli, R. Cerchione, E. Oropallo, and E. Riccio, ‘Blockchain Technology for Embracing Healthcare 4.0’, *IEEE Trans. Eng. Manag.*, vol. 70, no. 8, pp. 2998–3009, Aug. 2023, doi: 10.1109/tem.2022.3212007.
[31] S. V, D. Santhosh, S. C, S. N, G. Raja D, and A. Maran M, ‘Electronic Health Records Reimagined: A Blockchain Approach Combined with IPFS and Brain Tumor Detection Through Machine Learning’, in *2024 International Conference on Smart Systems for Electrical, Electronics, Communication and Computer Engineering (ICSSEECC)*, Coimbatore, India: IEEE, June 2024, pp. 315–320. doi: 10.1109/icsseecc61126.2024.10649457.
[32] L. V. Nguyen, ‘Recommendation Systems in Healthcare: Challenges, Limitations, and Its Applications’, in *2024 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, Danang, Vietnam: IEEE, Nov. 2024, pp. 1–4. doi: 10.1109/icce-asia63397.2024.10773682.
[33] M. Pedrosa, R. Lebre, and C. Costa, ‘A Performant Protocol for Distributed Health Records Databases’, *IEEE Access*, vol. 9, pp. 125930–125940, 2021, doi: 10.1109/access.2021.3111008.
[34] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, ‘Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology’, *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 1, Dec. 2020, doi: 10.1186/s12911-020-01275-y.
[35] D. Kumari, A. S. Parmar, H. S. Goyal, K. Mishra, and S. Panda, ‘HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy preserving scalable health data’, *Comput. Netw.*, vol. 241, p. 110223, Mar. 2024, doi: 10.1016/j.comnet.2024.110223.
[36] B. Ferik *et al.*, ‘A Multi-Layered Security Framework for Medical Imaging: Integrating Compressed Digital Watermarking and Blockchain’, *IEEE Access*, vol. 12, pp. 187604–187622, 2024, doi: 10.1109/access.2024.3514668.

[37] J.-H. Horng, C.-C. Chang, G.-L. Li, W.-K. Lee, and S. O. Hwang, 'Blockchain-Based Reversible Data Hiding for Securing Medical Images', *J. Healthc. Eng.*, vol. 2021, pp. 1–22, May 2021, doi: 10.1155/2021/9943402.
[38] G. Wu, S. Wang, Z. Ning, and B. Zhu, 'Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System', *IEEE J. Biomed. Health Inform.*, vol. 26, no. 5, pp. 1917–1927, May 2022, doi: 10.1109/jbhi.2021.3123643.
[39] F. Li, K. Liu, L. Zhang, S. Huang, and Q. Wu, 'EHRChain: A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem', *IEEE Trans. Serv. Comput.*, vol. 15, no. 5, pp. 2755–2765, Sept. 2022, doi: 10.1109/tsc.2021.3078119.
[40] 'Introduction to MyHealth@EU'. Accessed: July 20, 2025. [Online]. Available: https://www.ehealthireland.ie/technology-and-transformation-functions/standards-and-shared-care-records-sscr/myhealth-eu/introduction-to-myhealth-eu/
[41] 'Keyless Signature Infrastructure'. Accessed: July 20, 2025. [Online]. Available: https://m.guardtime.com/files/KSI_data_sheet_201509.pdf
[42] 'Estonian e-Health Records', e-Estonia. Accessed: July 20, 2025. [Online]. Available: https://e-estonia.com/solutions/e-health-2/e-health-records/
[43] 'X-Road®', X-Road®. Accessed: July 20, 2025. [Online]. Available: https://x-road.global
[44] 'PLA - Digital Trust Ecosystem', PharmaLedger Association. Accessed: July 20, 2025. [Online]. Available: https://pharmaledger.org/
[45] 'Horizon 2020 - European Commission'. Accessed: July 20, 2025. [Online]. Available: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en
[46] 'Innovative Health Initiative | IHI Innovative Health Initiative'. Accessed: July 20, 2025. [Online]. Available: http://www.ihi.europa.eu/
[47] 'Power Future-Ready Solutions with the LifeGraph® Platform'. Accessed: July 20, 2025. [Online]. Available: https://burstiq.com/
[48] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, 'A Design Science Research Methodology for Information Systems Research', *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.
[49] 'Internet Protocol', Internet Engineering Task Force, Request for Comments RFC 791, Sept. 1981. doi: 10.17487/RFC0791.
[50] NEMA, 'DICOM Standard, Part 18: Web Services'. Accessed: Dec. 20, 2025. [Online]. Available: https://dicom.nema.org/medical/dicom/current/output/chtml/part18/chapter_6.html
[51] European Telecommunications Standards Institute, 'ETSI EN 319 401 V2.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers', 2016, Accessed: Oct. 20, 2025. [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf
[52] 'Home - EBSI -'. Accessed: Dec. 20, 2025. [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/447687044/Home
[53] M. N. Alruwaill, S. P. Mohanty, and E. Kougianos, 'hChain 4.0: A Secure and Scalable Permissioned Blockchain for EHR Management in Smart Healthcare', 2025, *arXiv*. doi: 10.48550/ARXIV.2505.13861.
[54] 'Guidelines 02/2025 on processing of personal data through blockchain technologies | European Data Protection Board'. Accessed: Dec. 20, 2025. [Online]. Available: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en
[55] *EN ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, Brussels., 2022. Accessed: Oct. 21, 2025. [Online]. Available: https://www.iso.org/standard/27001

[56] *EN ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*, Brussels., 2025. Accessed: Oct. 21, 2025. [Online]. Available: https://www.iso.org/standard/27701

[57] D. Hardt, A. Parecki, and T. Lodderstedt, 'The OAuth 2.1 Authorization Framework', Internet Engineering Task Force, Internet Draft draft-ietf-oauth-v2-1-14, Oct. 2025. Accessed: Dec. 20, 2025. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-oauth-v2-1

[58] 'User-Managed Access (UMA) Profile of OAuth 2.0'. Accessed: Dec. 20, 2025. [Online]. Available: https://docs.kantarainitiative.org/uma/rec-uma-core.html

[59] *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*, vol. 151. 2019. Accessed: Dec. 20, 2025. [Online]. Available: http://data.europa.eu/eli/reg/2019/881/oj

[60] H. K. Huang, *PACS and imaging informatics: basic principles and applications*, 2nd ed. Hoboken, N.J: Wiley-Blackwell, 2010. Accessed: Oct. 20, 2025. [Online]. Available: https://www.wiley.com/en-us/PACS%2Band%2BImaging%2BInformatics%3A%2BBasic%2BPrinciples%2Band%2BApplications%2C%2B2nd%2BEdition-p-x000443107 Wiley

[61] R. T. Fielding and J. Reschke, 'Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content', Internet Engineering Task Force, Request for Comments RFC 7231, June 2014. doi: 10.17487/RFC7231.

[62] Roy Thomas Fielding, 'Architectural Styles and the Design of Network-based Software Architectures', University of California, Irvine, 2000. Accessed: Dec. 20, 2025. [Online]. Available: https://dl.acm.org/doi/book/10.5555/932295

[63] E. Rescorla, 'The Transport Layer Security (TLS) Protocol Version 1.3', Internet Engineering Task Force, Request for Comments RFC 8446, Aug. 2018. doi: 10.17487/RFC8446.

[64] B. Beyer, C. Jones, J. Petoff, and N. R. Murphy, Eds, *Site reliability engineering: how Google runs production systems*, First edition. Beijing Boston Farnham Sebastopol Tokyo: O'Reilly, 2016. Accessed: Oct. 21, 2025. [Online]. Available: https://dl.acm.org/doi/book/10.5555/3006357

[65] European Parliament. Directorate General for Parliamentary Research Services., *Blockchain and the general data protection regulation: can distributed ledgers be squared with European data protection law?* LU: Publications Office, 2019. Accessed: Dec. 20, 2025. [Online]. Available: https://data.europa.eu/doi/10.2861/535

[66] 'eHealth Network - Public Health - European Commission'. Accessed: Dec. 20, 2025. [Online]. Available: https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/eu-cooperation/ehealth-network_en

[67] *EN ISO 22301:2019 — Security and resilience — Business continuity management systems — Requirements*, Geneva, Switzerland., 2019. Accessed: Oct. 21, 2025. [Online]. Available: https://www.iso.org/standard/75106.html

APPENDICES

APPENDIX A - FR/NFR TRACEABILITY AND EVIDENCE BUNDLE

Table 17 - Functional requirements traceability: component, standard, journey, evidence.

ID	Requirement	Architectural component(s)	Standard or profile anchors	Journey coverage	Verifiable evidence at design-time
FR-01	Secure Image Management	Patient wallet; Off-chain encrypted storage; DICOMweb interface	DICOMweb (QIDO-RS/WADO-RS/STOW-RS); FHIR ImagingStudy or DocumentReference.	J1	Encrypted object stored off-chain; salted integrity digest anchored on the ledger with tx id and timestamp; FHIR resource id; upload AuditEvent id.
FR-02	Granular Consent Management	Consent smart contract; Access gateway; Wallet consent UI	FHIR Consent; OAuth 2.1 or UMA token with scope/audience/TTL; DID/VC for actor attributes.	J1 (self-view), J2, J3	Consent state with purpose, audience, scope, and validity; scoped token claims; allow/deny AuditEvent outcomes tied to consent state.
FR-03	Cross-Border Sharing	Interoperability layer; Access gateway; Identity and trust services	EEHRxF alignment; MyHealth@EU payload expectations; FHIR ImagingStudy/DocumentReference for metadata; DICOMweb WADO-RS for pixel data; eIDAS-aligned identity presentation.	J2	Consent-grant tx id and FHIR Consent id; issued token or issuance log bound to audience and purpose; AuditEvent allows within scope and time.
FR-04	Auditability and Transparency	Audit and provenance module; Ledger anchor	FHIR AuditEvent and Provenance; IHE ATNA (Audit Trail and Node Authentication); on-chain audit anchor of policy state.	J1–J4; J4 central	Time-ordered reconstruction possible from linked Consent/Provenance/AuditEvent; signed evidence bundle; reference to consent-state anchor.
FR-05	Secure Authentication & Identity Management	Identity and trust services; Wallet auth; Provider auth	eIDAS assurance; W3C DID/VC; OIDC/OAuth for session; IHE XUA where applicable	J2–J4	Verifiable presentation or assertion with role/assurance; session record; AuditEvent actor fields reflecting verified identity.
FR-06	Interoperability with European Standards	Interoperability layer; API façade	FHIR REST; DICOMweb; EEHRxF datasets; EIF modularity.	J1–J4	Conformance statement for chosen FHIR/DICOM profiles; successful flow using only those resources; standard IDS present in artefacts.

Table 18 - Non-functional requirements traceability: design mechanism, component, evidence.

ID	Requirement	Design mechanism or SLO	Architectural component(s)	Verifiable evidence at design-time
NFR-01	GDPR Compliance	Privacy by design; no personal data concerning health or stable identifiers on-chain; rights enablement; DPIA sketch	Data placement policy; Consent and ledger layer; Wallet export and deletion flows	Table 13 design-time guarantees; 4.4.1 DPIA sketch; demonstration of off-chain erasure and on-chain state change records
NFR-02	Scalability	Off-chain object storage; horizontal scaling; no large payloads on ledger	Off-chain storage; Interoperability layer	Architectural rationale explaining storage and request patterns; absence of large on-chain payloads
NFR-03	Interoperability	Use only DICOMweb for images and FHIR for metadata; align with EEHRxF/MyHealth@EU	Interoperability layer	Section 3.4 interoperability and legal mapping; J1–J4 instantiating FHIR and DICOMweb resources exclusively; standards-conformant interaction and error handling.
NFR-04	Availability & Reliability	Target ≥ 99.9% for consent/audit planes; redundancy and failover; monitoring	Resilience and monitoring; Access gateway; Ledger nodes	Design-time SLOs in 4.2.3.2; redundancy and failover design; health check and alerting assumptions
NFR-05	Data Integrity & Security	Client-side encryption; salted digests anchored; key custody with patient	Cryptographic services; Ledger anchor	Presence of integrity digest on-chain; encryption described; no plaintext personal health data in any ledger artefact
NFR-06	Usability & Accessibility	Mobile-first; clear copy; WCAG-aware patterns	Patient wallet UI	Journey mockups in 4.5; UI affordances and captions informed by accessibility conventions
NFR-07	Performance & Response Time	P95 consent verification ≤ 2 seconds; revocation propagation ≤ 5 seconds	Access and authorisation path; Consent contract	Design-time targets cited in 4.2.3.2; no conflicting assumptions in flows; acknowledgement under 4.8 limitations

Table 19 - Minimal evidence bundle fields.

Field	Description	Source system	Storage location
request_id	Correlates an access decision or action	Access gateway or audit service	Included in bundle; referenced in AuditEvent
subject_handle	Pseudonymous patient handle used in logs	Wallet or audit viewer	Included in bundle; not on-chain
scope_code	Encodes study or collection within consent scope	Consent state and token claims	Included in bundle and token issuance log
purpose_code	Declared purpose of use	Consent resource	Included in bundle and AuditEvent
consent_state_hash	Non-identifying anchor of the policy state	Ledger contract	Bundle includes the hash and ledger transaction id
decision	Allow or deny outcome with reason when applicable	AuditEvent outcome	Included in bundle
ts_qualified	Qualified time or trusted timestamp reference	Trust service or ledger	Included in bundle
signer	Identity of the entity that signs the bundle or decision record	Wallet, gateway, or auditor	Digital signature over bundle metadata

Table 20 - Mapping of system requirements to European standards and regulations

Requirement Type	Requirement / Functionality	GDPR Mapping	eIDAS Mapping	FHIR Mapping	DICOM / DICOMweb Mapping	EEHRxF Mapping
Functional	Secure image management	Art. 9; Art. 32; Art. 5(1)(f); Art. 25	N/A	ImagingStudy; DocumentReference; Endpoint; Binary (optional)	DICOM PS3; DICOMweb QIDO-RS/WADO-RS/STOW-RS; IHE XDS-I.b/MHD	EEHRxF priority dataset: medical imaging studies and related imaging reports; MyHealth@EU imaging service (NCPeH); eHN imaging guideline.
Functional	Granular consent management	Art. 7; Art. 7(3); Art. 9(2)(a); Art. 6(1)(a) where consent is the lawful basis	N/A	Consent; Provenance; AuditEvent	N/A	N/A (EEHRxF specifies exchange datasets; the EHDS/MyHealth@EU policy layer handles consent).
Functional	Cross-border sharing	Art. 20; Art. 15; Art. 26 or Art. 28 (as applicable); Arts. 44–49 only if a third country/organisation outside the EEA is involved	Arts. 6–12 (mutual recognition of notified eID), esp. Art. 8 (assurance levels).	Bundle; DocumentReference; ImagingStudy; Provenance	DICOM PS3.18 (QIDO-RS/WADO-RS); IHE XCA/XDS-I.b (where document-based exchange is used)	MyHealth@EU/NCPeH cross-border service; EEHRxF-conformant imaging study/report exchange (eHN imaging guideline).
Functional	Auditability and transparency	Art. 5(2); Art. 24; Art. 30; Art. 12–14	Arts. 25, 35, 41–42 (qualified e-signature, e-seal and e-time stamp as evidence)	AuditEvent; Provenance	DICOM PS3.15 (audit message format); IHE ATNA	MyHealth@EU governance and traceability expectations for primary-use exchanges.
Functional	Secure authentication and identity management	Art. 32; Art. 5(1)(f); Art. 25	Art. 5a (EUDI Wallet) and/or Arts. 6–12 (notified eID); add Art. 45g only if you model roles as electronic attestations of attributes.	CapabilityStatement (rest.security)	DICOMweb over HTTP/TLS; IHE ATNA; IHE XUA (if SAML assertions are used)	MyHealth@EU trust framework for primary-use exchanges (NCPeH).
Functional	Interoperability with European standards	Art. 20; Art. 15; Art. 5(1)(f)	N/A	Core RESTful APIs; profiles and terminology bindings	DICOM PS3; DICOM PS3.18 (DICOMweb); IHE profiles as applicable	EEHRxF conformance to EU profiles, terminologies and priority datasets (incl. imaging studies/reports).
Non-Functional	GDPR compliance	Art. 5; Art. 6; Art. 9; Art. 12–22; Art. 25; Art. 28; Art. 30; Art. 32; Art. 35; Arts	N/A	N/A	N/A	Supports EHDS/EEHRxF primary-use exchange with data minimisation (no personal data on-chain).
Non-Functional	Scalability	Art. 32; Art. 25	N/A	Pagination; search; async operations	QIDO-RS paging (limit/offset); WADO-RS bulk/frames retrieval	Supports EEHRxF imaging exchange at scale (large study lists; filtered query and retrieval).
Non-Functional	Interoperability with health systems	Art. 20; Art. 15	N/A	Standard RESTful FHIR exchange	DICOM DIMSE (C-FIND/C-MOVE/C-STORE) and/or DICOMweb; IHE MHD/XDS-I.b	Cross-border semantic and structural alignment with EEHRxF/MyHealth@EU.
Non-Functional	Availability and reliability	Art. 32(1)(b); Art. 32(1)(c); Art. 32(1)(d)	N/A	CapabilityStatement (/metadata); retry semantics	HTTP status codes; idempotent QIDO-RS/WADO-RS retries; STOW-RS response semantics	Supports continuity-of-care availability expectations for MyHealth@EU services.
Non-Functional	Data integrity and security	Art. 5(1)(f); Art. 32; Art. 25; Art. 33–34 (incident-related)	Arts. 25, 35, 41–42 (integrity and time evidence via qualified signature, seal and time stamp).	Provenance; AuditEvent	DICOM PS3.15 (security profiles, digital signatures); DICOMweb over HTTP/TLS	Supports trustworthy MyHealth@EU/EEHRxF primary-use exchanges.
Non-Functional	Usability and accessibility	Art. 12; Art. 12(2); Art. 12(3)	N/A	Human-readable artefacts; patient-facing resources	N/A	Supports patient and professional access scenarios envisaged by EHDS/EEHRxF (incl. imaging).
Non-Functional	Performance and response time	Art. 32 where tied to availability/resilience; Art. 12(3) only where tied to response times for data subject requests	N/A	Optimised queries/search; conditional requests; _summary/_elements	WADO-RS frames/renditions; QIDO-RS query filters; STOW-RS multipart upload	Supports timely request and retrieval workflows for MyHealth@EU imaging exchange.

APPENDIX B - ARCHITECTURAL DECISION RECORDS

Table 21 - Architectural Decision Records (accepted)

ADR ID	Decision	Summary justification	Key implications	Trace (FR/NFR)
ADR-01	Consent is evaluated at the time of the request, with a single live state.	Deterministic authorisations and immediate revocation without reissuing artefacts.	Every DICOMweb/FHIR request passes through the gateway, which issues or rejects short-lived capabilities.	FR-02, FR-03; NFR-04, NFR-07
ADR-02	Permissioned consortium ledger operated by accredited healthcare entities.	Requirements of trust, audit and governance.	Membership, change control and incidents formalised; timely finalisation by consensus.	FR-02, FR-04; NFR-04
ADR-03	No clinical content or direct identifiers are recorded on the chain.	GDPR minimisation and support for erasure.	The chain stores only salted commitments and policy statements; pixels/CIDs/stable IDs remain off-chain.	FR-01, FR-02, FR-04; NFR-01, NFR-05
ADR-04	Encrypted off-chain storage for DICOM objects.	Scalability and confidentiality for extensive studies.	Client-side encryption, residence in the EU/EEA, retrieval via DICOMweb; verification by digest.	FR-01; NFR-01, NFR-02, NFR-05
ADR-05	High-assurance identity with DIDs and verifiable credentials.	Cross-border portability and strong role binding.	Patients and providers authenticate using DID/VC; aligned with eIDAS.	FR-05, FR-03; NFR-05
ADR-06	Interoperability interface: FHIR for metadata and DICOMweb for images.	Reduces integration effort and aligns with EU practice.	Discovery, consent and audit are handled via FHIR; query, retrieve, and store operations use QIDO/WADO/STOW.	FR-01, FR-03, FR-06; NFR-03
ADR-07	Short-lived tokens bound to the recipient, including a nonce and an optional proof of possession.	Mitigates replay and token theft.	Claims encode scope, audience and expiry; each request has a unique value; binding to the caller's key is supported when available.	FR-03, FR-05; NFR-05, NFR-07
ADR-08	Auditing with FHIR AuditEvent and Provenance, anchored to the chain.	Readable by the patient and the regulator with immutable anchors.	Full records remain in FHIR; the chain stores non-identifying anchors for states and milestones.	FR-04; NFR-05
ADR-09	Emergency access is strictly limited, recorded, and reviewed.	Vital needs when consent is not available.	A separate authorisation route with purpose codes, minimum scope, notifications, and review.	FR-02; NFR-05, NFR-04
ADR-10	Design SLOs define service quality and are not measured here.	Analytical evaluation in this thesis, with empirical validation later.	Targets for consent latency, revocation propagation and availability guide sizing and caching.	NFR-04, NFR-07
ADR-11	Consortium governance with supermajority finalisation and independent audit.	Security, liveness and accountability.	Validator compliance, changes, and incidents are recorded and reviewed periodically.	NFR-04
ADR-12	Client-side encryption and patient-centred key custody.	Confidentiality and user control.	Keys are generated on the client, separated by function, rotated on lifecycle events, and never stored on the chain.	NFR-01, NFR-05
ADR-13	Minimal verifiable evidence set without exposing health data.	Verifiability with privacy.	The evidence bundle includes correlation, pseudonym, scope and purpose codes, decision, qualified time, signer and state anchor.	FR-04; NFR-01, NFR-05

Table 22 - Deferred ADRs (for future implementation/validation).

ADR ID	Deferred topic	Reason for deferral	Suggested next step	Trace (FR/NFR)
ADR-D1	Specifics of national connectors and variations in code systems (NCPeH)	Variability across Member States	Profiling during implementation while maintaining the FHIR/DICOMweb interface	FR-03, FR-06; NFR-03
ADR-D2	Consent granularity at the series level and multi-modality studies	Requires validation with PACS/VNA	Trials in partner testbeds; profiling if necessary	FR-02
ADR-D3	Usability and accessibility testing with diverse populations	Requires user studies	Planning formal studies; UI/UX adjustments	NFR-06
ADR-D4	Post-quantum crypto agility and migration strategies	Awaiting EU guidance and maturity	Migration and re-anchoring plans when applicable	NFR-05

APPENDIX C – ARCHITECTURAL ASSUMPTIONS AND MODULE–STANDARDS MAPPINGS

Table 23 - Design-time assumptions and constraints

Area	Assumptions (expected to hold)	Constraints (imposed by the design)	Rationale and implication
Identity and trust	High-assurance identities for clinical actors; verifiable credentials can be issued and verified; endpoints use qualified certificates with mutual TLS.	No anonymous provider access; emergency access only for authenticated clinical roles, with reason capture.	Enables portable, accountable access decisions across borders; narrows break-glass to a controlled path.
Ledger governance	Permissioned consortium ledger with a published charter; supermajority finality within seconds; independent audit of validators.	No clinical content or personal identifiers on-chain; only salted commitments and consent policy statements; public L1 chains and tokenomics excluded.	Provides tamper-evident consent provenance without creating a secondary health data store.
Data placement and storage	Encrypted off-chain storage hosted in the EU/EEA; content-addressable or equivalent integrity guarantees; patient key custody preferred.	DICOM instances never on-chain; stable identifiers and resolvable content addresses are not written to the ledger; erasure via key/pointer rotation, not on-chain mutation.	Preserves GDPR minimisation while maintaining verifiable integrity.
Interoperability surface	DICOMweb for pixel data; FHIR for metadata, consent, provenance and audit; alignment with EEHRxF payloads and error semantics.	No workflow orchestration or reporting pipelines; no proprietary gateway protocols; national connector specifics out of scope.	Focuses the PoC on discovery, consent and viewing, easing partner onboarding.
Authorisation path	A single access gateway mediates all DICOMweb and FHIR requests; the live consent state is the single source of truth.	Deny-by-default for ambiguity; short-lived, audience-bound tokens or introspection on every request; no side-channel file exchange.	Enforces determinism for allow/deny and simplifies security analysis.
Security controls	Hardware-backed keys when available; modern ciphers (AEAD); nonce discipline; replay resistance; rate-limiting and uniform errors.	Private keys are never on-chain; pseudonyms rotate; detailed AuditEvent remains off-chain, with an on-chain anchor only.	Reduces replay/linkability risks while maintaining a comprehensive audit and preserving privacy.
Availability and performance	Consent checks typically complete within a short user-interaction cycle; revocation propagates across the consortium within seconds; quorum finality bounds are known.	Chapter 3 lacks empirical benchmarking; the design must not rely on long-lived bearer tokens or stale caches.	Provides realistic targets for sizing and cache strategy; measurements are deferred to later work.
Compliance and hosting	Processing is confined to the EU/EEA; the routine lawful basis is explicit consent; emergency uses are based on vital interests, with retrospective review.	Third-country transfers, complex joint-controller arrangements, and nuances of nationwide connectors are excluded at this stage.	Keeps the legal model simple and evaluable, without deployment-specific variations.
Usability and accessibility	Mobile-first wallet, clear copy, WCAG-aware patterns; multilingual affordances feasible.	Key recovery and delegation patterns are outlined but not validated with end users here.	Maintains patient control while recognising the need for usability trials.
Implementation neutrality	Multiple conformant components are possible per module (ledger, wallet, FHIR/DICOM servers).	No vendor-specific features required; cryptocurrencies, NFTs, and economic incentives excluded.	Avoids lock-in and keeps the PoC reproducible.

Table 24 - Architecture module mapping.

Component	Technology Class	Standards	Exemplary Options	Role in the Architecture
Patient Wallet Module	Digital identity wallet with key management	eIDAS and EUDI Wallet (EUDI ARF), W3C DID and Verifiable Credentials, OpenID4VP and OpenID4VCI	EUDI Reference Wallet codebases; Aries Bifold-based wallet; walt.id wallet SDK; OpenID4VP/OpenID4VCI libraries	User-facing app for uploading, viewing, and sharing images; managing consent and keys under patient control
Blockchain Network Module	Permissioned distributed ledger with smart contracts	GDPR (data minimisation, privacy by design), EBSI alignment, ETSI EN 319 4xx (trust service standards for signatures, seals, time stamps)	Hyperledger Besu; Hyperledger Fabric; Quorum; Corda	Record non-identifying metadata and consent states; enforce policies via smart contracts; provide tamper-evident audit anchors
Off-Chain Storage Module	Distributed and encrypted object storage	DICOM and DICOMweb (QIDO-RS, WADO-RS, STOW-RS), IHE XDS-I.b and IHE MHD	IPFS Cluster with EU/EEA pinning; S3-compatible object storage (MinIO, Ceph RGW); Orthanc DICOMweb; dcm4chee DICOM archive	Store encrypted DICOM objects; expose content addresses; anchor hashes/commitments on-chain
DID Services Module	DIDs and verifiable credentials	W3C DID and Verifiable Credentials, eIDAS and EUDI Wallet framework, EU Trusted Lists (eIDAS trust lists)	did:ebsi; did:web; Aries/Indy agent components; Veramo; walt.id issuer and verifier services	Authenticate patients and providers; issue and verify VCs for cross-border identity and attributes.
Access Requester Interfaces Module	Interoperability APIs for clinical systems	HL7 FHIR, DICOMweb, EEHRxF, MyHealth@EU and NCPeH profiles/guidelines	HAPI FHIR; Firely Server; SMART on FHIR client apps; DICOMweb gateways (Orthanc, dcm4chee)	Enable hospitals/clinics to request patient-approved data, check consent, and retrieve imaging and metadata.
Audit and Provenance Module	Immutable, standards-based event logging	GDPR (accountability and records of processing), HL7 FHIR AuditEvent and Provenance, IHE ATNA	FHIR server AuditEvent and Provenance services (HAPI, Firely); ATNA audit repository via syslog-ng/rsyslog; on-chain audit anchor contract	Record and verify access and consent events; expose regulator- and patient-readable audit trails
Access Gateway Module	Authorisation and token issuance	OAuth 2.1, OIDC, UMA 2.0, SMART on FHIR, aligned with MyHealth@EU and EUDI Wallet flows	Keycloak; Curity; WSO2 Identity Server; ForgeRock Access Management	Broker access between requesters and wallet/storage; issue short-lived tokens aligned with consent
Cryptographic Services Module	End-to-end encryption and secure key custody	ENISA guidance on cryptography and key management, ETSI EN 319 4xx where qualified trust services apply, CEN/CENELEC secure element and trust-service assurance practices	OpenSSL; libsodium; BouncyCastle; PKCS#11 with SoftHSM; HSMs (Thales, Utimaco); platform TEE (TPM, SGX, TrustZone)	Provide encryption, hashing, key generation and rotation, and secure exchange for all modules
Resilience and Monitoring Module	Reliability, observability, and recovery	NIS2 Directive alignment, ENISA incident handling guidance, EN ISO/IEC 27001 and EN ISO/IEC 27701, EN ISO 22301 [67]	Prometheus; Grafana; OpenSearch or Elastic Stack; Loki; Jaeger; Kubernetes with Velero backups	Ensure high availability, detect anomalies, and support backup and restore, as well as incident response

Table 25 - Actors and Trust Boundaries.

Actor	Role and Responsibility	Trust Boundary
Patient	- Uploads medical imaging data (e.g., DICOM images) to the wallet. - Grants or revokes consent for data sharing. - Views audit logs and consent history.	- Data at rest: Patient images are stored in encrypted off-chain storage. - Data in transit: Secure end-to-end encryption for data during sharing. - Consent control: Managed via smart contracts.
Healthcare Providers	- Accesses imaging data for clinical use, respecting the patient's consent. - Includes doctors, nurses, and other medical professionals. - Ensures data is accessed securely and only in accordance with consent.	Data access: Limited to images shared by the patient, in line with the scope of consent. - Identity: DIDs/VCs. - Access control: Based on patient consent and medical need.
Trusted Health Actors	- Manages the ledger. - Manages encryption keys. - Facilitates cross-border data exchange via secure gateways.	- Ledger interactions: Write and read access to the permissioned ledger, ensuring only authorised health actors can perform these actions. - Trust management: Identity verified via DIDs and secure gateway protocols.
Identity Providers (IDPs)	- Authenticate patient and healthcare provider identities. - Issue DIDs and VCs for trusted access.	- Identity management: Ensures secure and compliant identity creation and management. - Trust boundary: IDPs verify user identities without disclosing sensitive data.
Regulatory Authorities	- Ensure compliance with GDPR, eIDAS, and other relevant regulations. - Monitor the system for compliance with data protection and interoperability standards.	- Oversight: May have access to audit logs for compliance purposes. - Trust boundary: Regulatory bodies ensure that all activities within the system comply with the law.
Interoperability Gateways	- Facilitate data exchange between institutions by converting data into compliant formats (e.g., FHIR and DICOMweb).	- Data flow: Responsible for ensuring secure data exchange and validating cross-border health data transactions. - Trust boundary: Gateways ensure compliance with interoperability frameworks such as MyHealth@EU.
Insurance Providers	- Access patient imaging data to verify claims or to determine eligibility for coverage.	- Consent-controlled access: Data can be accessed only if the patient has granted consent to share. - Data privacy: Insurance data is managed in compliance with privacy regulations.
Data Custodians (Hospitals/Clinics)	- Store and manage imaging data, ensuring secure storage and retrieval.	- Data storage: Responsible for ensuring that medical images are safely stored off-chain and made accessible via the DICOMweb interface. - Access control: Responsible for granting access in line with consent.
Cross-border Service Providers	- Facilitate cross-border data exchange between institutions, ensuring compliance with cross-border standards (e.g., MyHealth@EU).	- Cross-border data sharing: Ensure data is transmitted securely across national borders. - Compliance: Ensure that the data exchange complies with both national and EU laws.
Audit and Compliance Entities	- Monitor and audit the system for regulatory compliance. - Ensure the system's security, transparency, and integrity in data sharing.	- Audit access: Ensure audit logs and interactions are maintained in a tamper-evident manner. - Trust boundary: Audit entities ensure compliance without disrupting the system's operation.

APPENDIX D – MOCKUPS OF USER JOURNEY

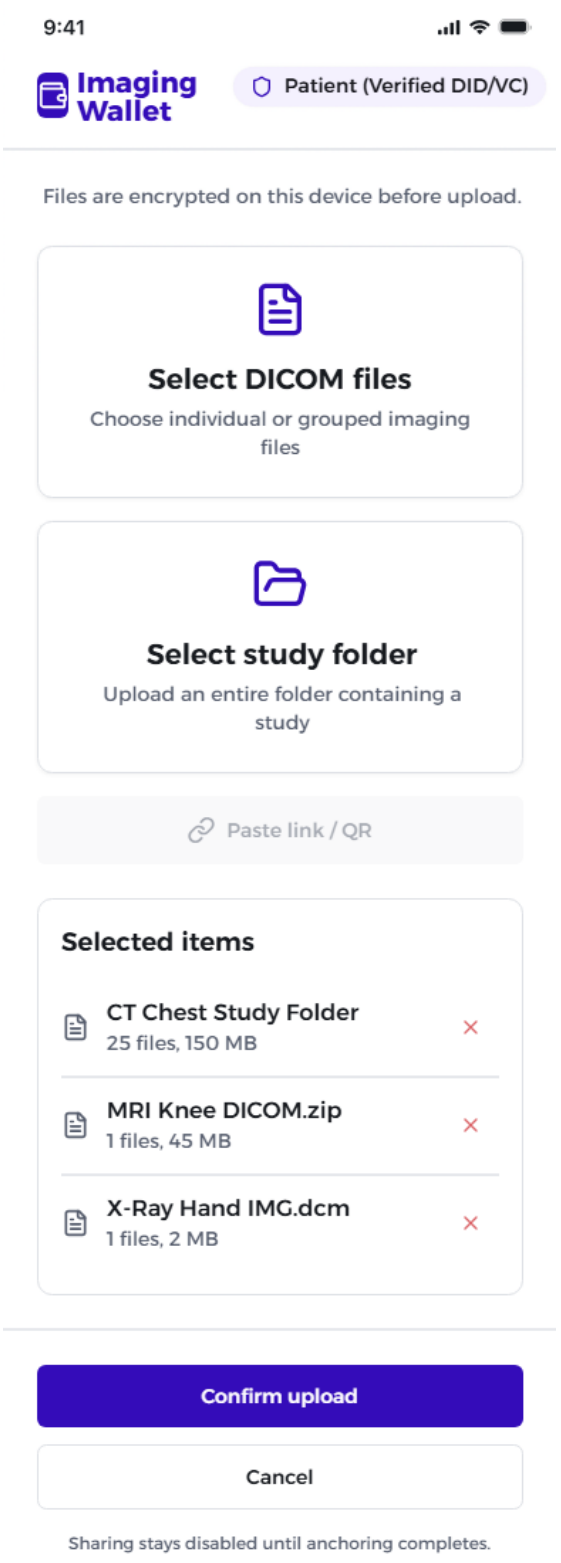


Figure 5 - Upload chooser and selection surface.

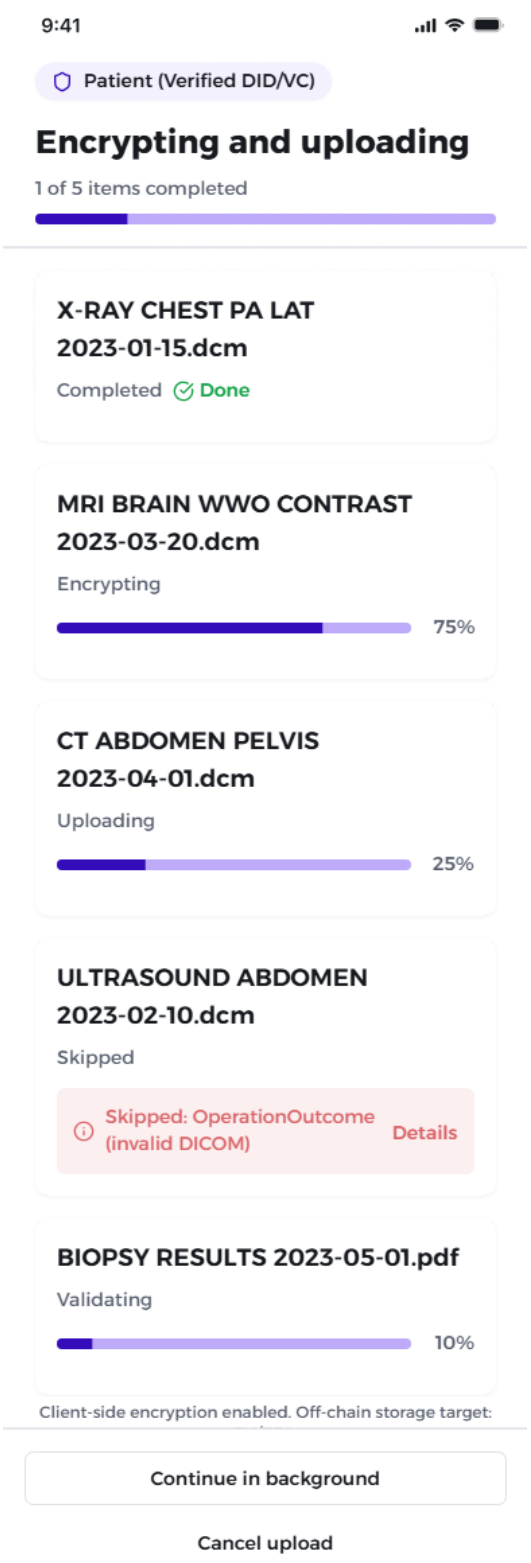


Figure 6 - Validation and client-side encryption progress.

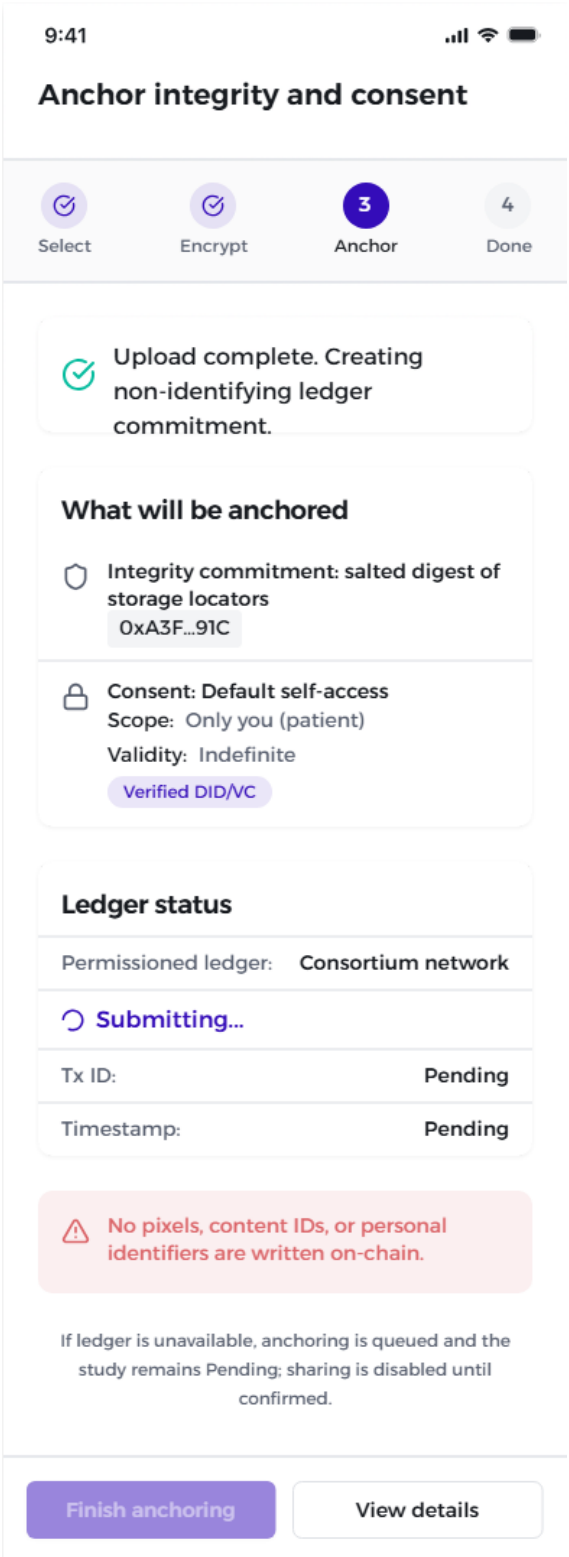


Figure 7 - Consent and integrity anchoring confirmation.

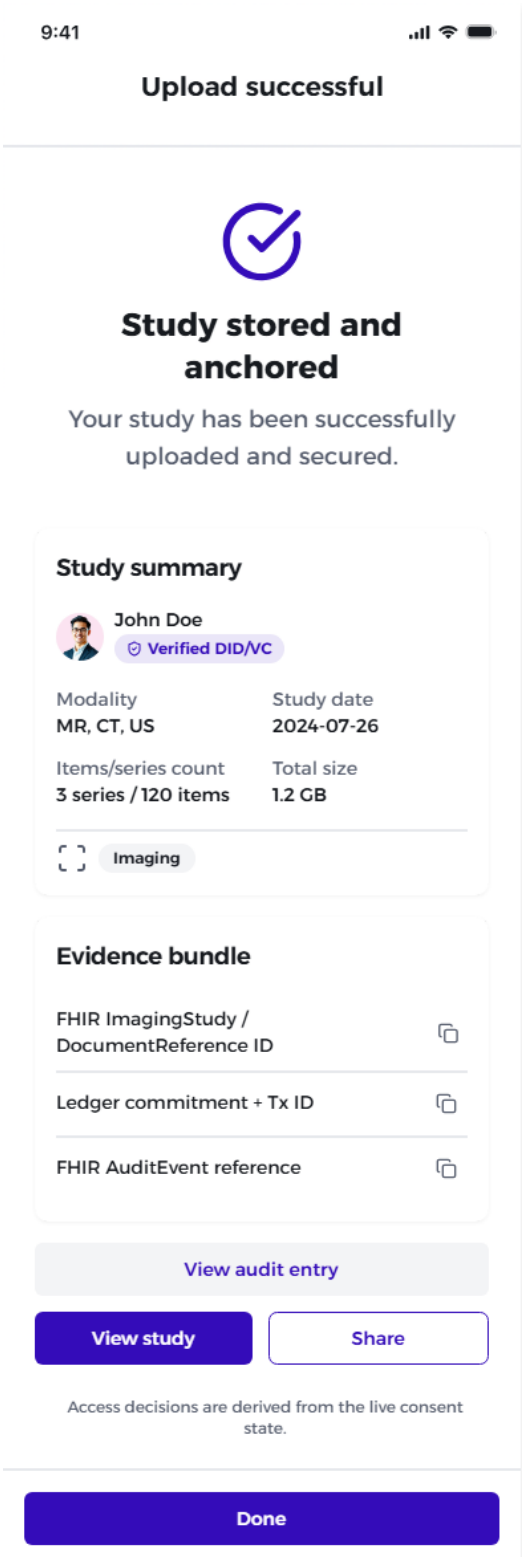


Figure 8 - Upload success, study summary and audit entry link.

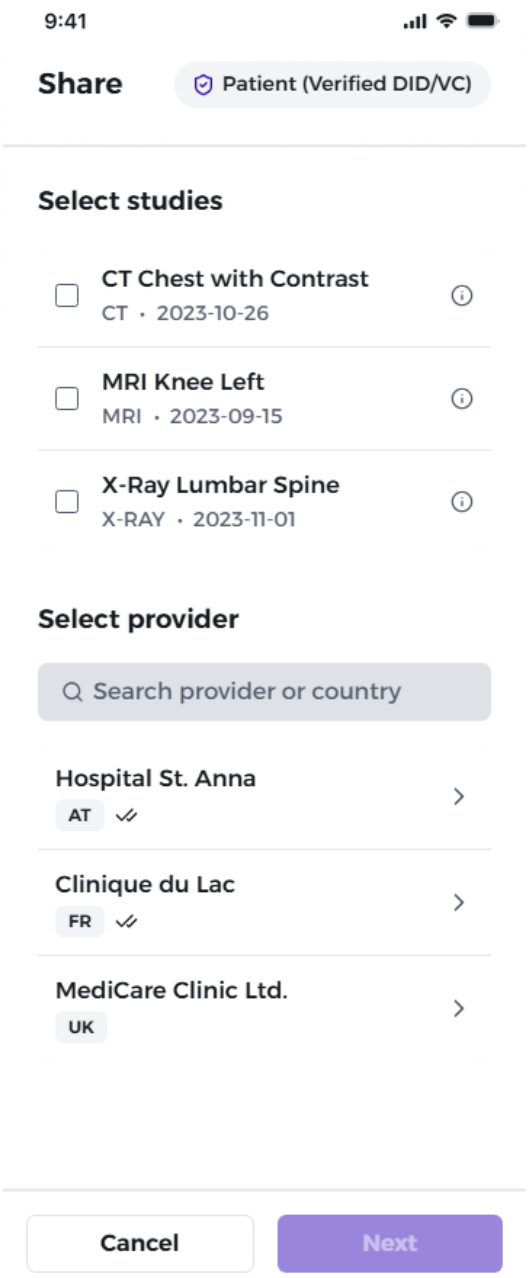


Figure 9 - Provider selection and study scope screen.

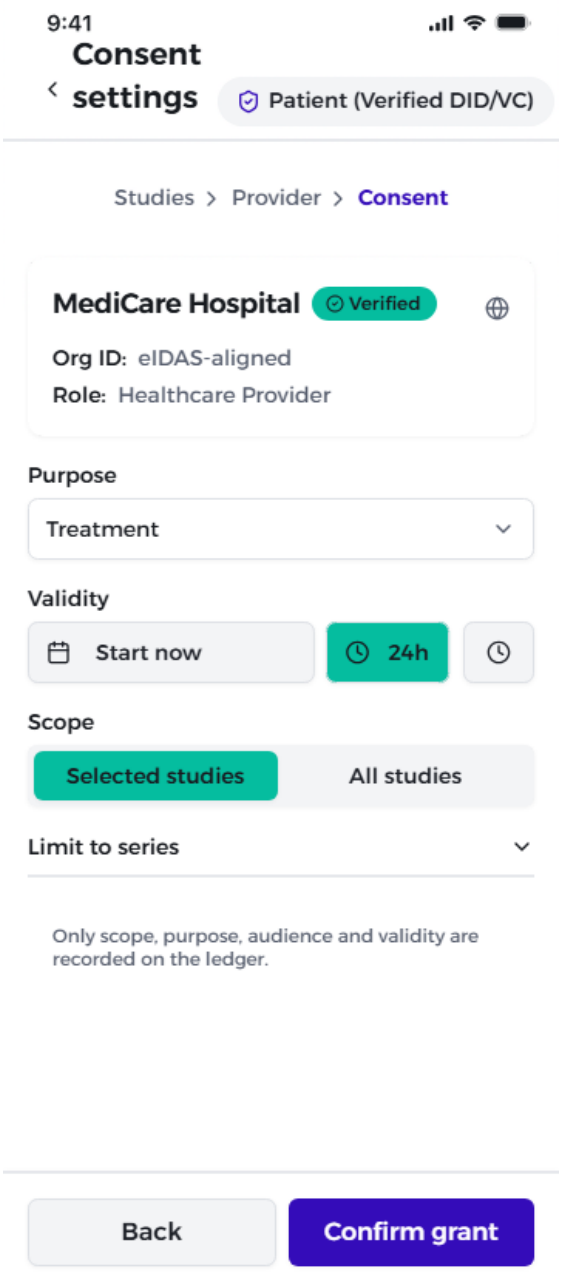


Figure 10 - Consent configuration with purpose, validity and verified provider identity.

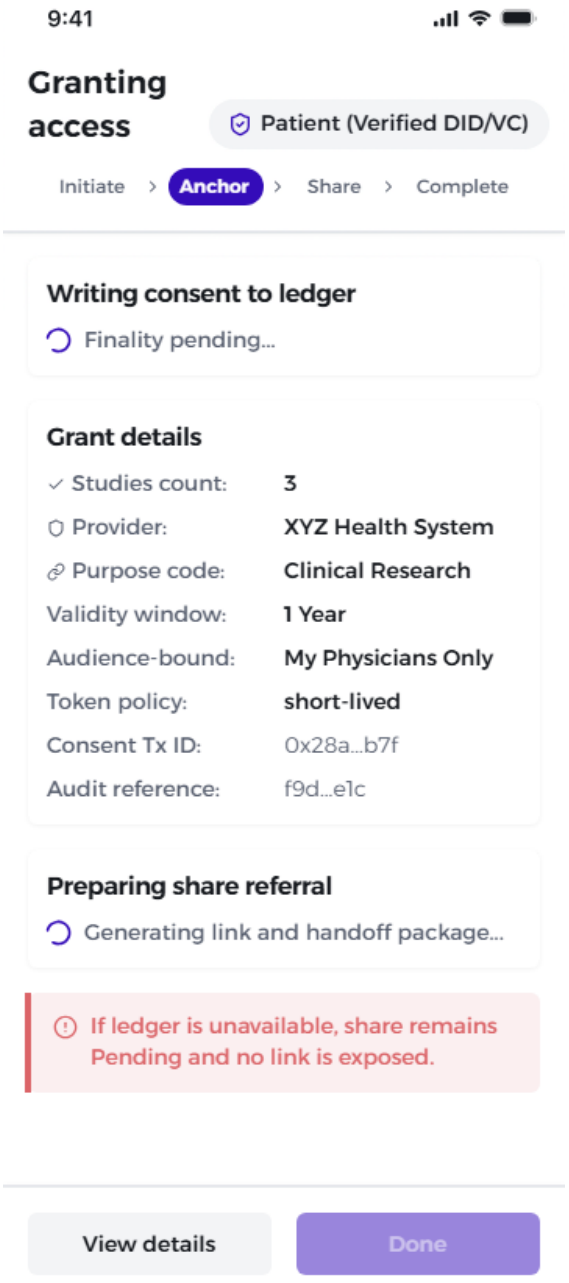


Figure 11 - Consent anchoring confirmation on ledger and share-link preparation.

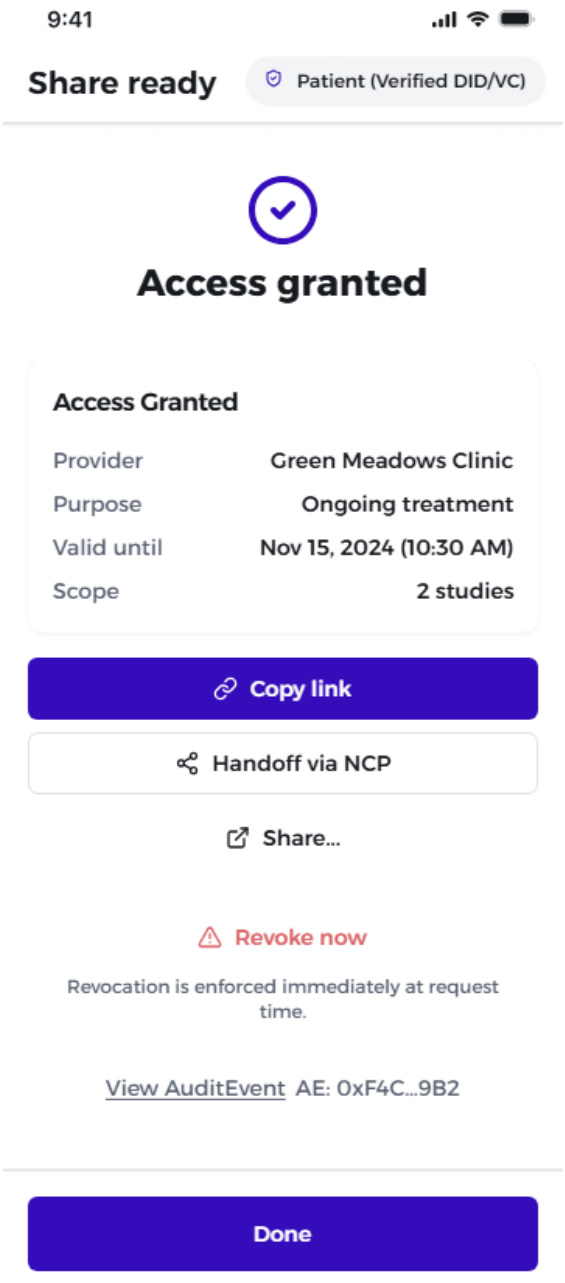


Figure 12 - Share the success summary with a copy link, handoff, and revoke control.

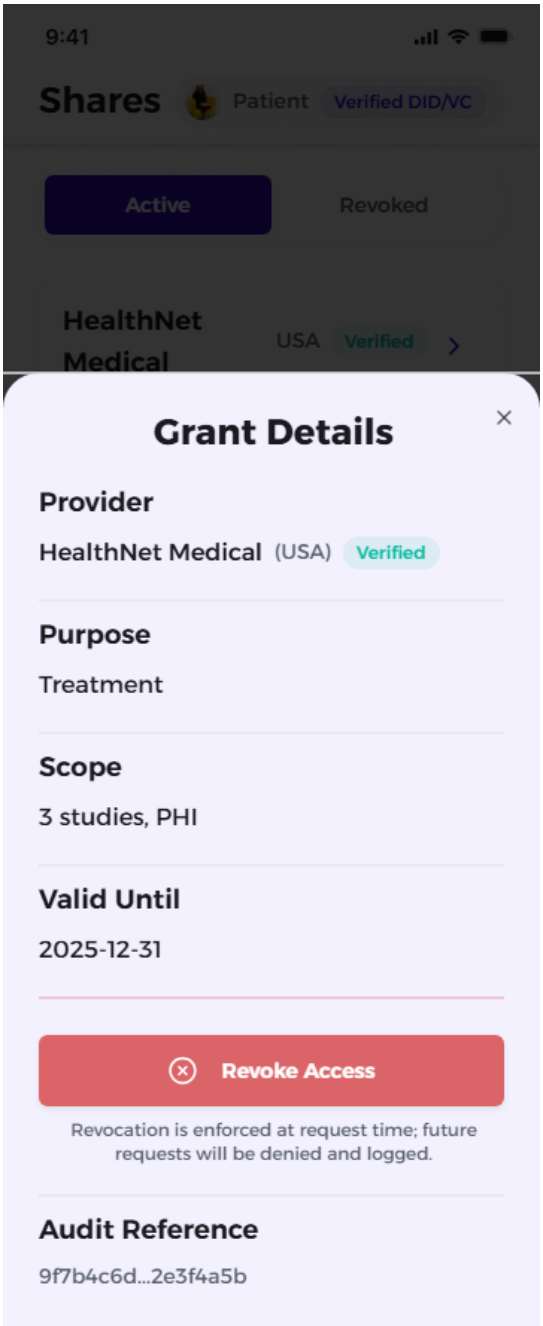


Figure 13 - Active shares list with per-grant detail and Revoke control.

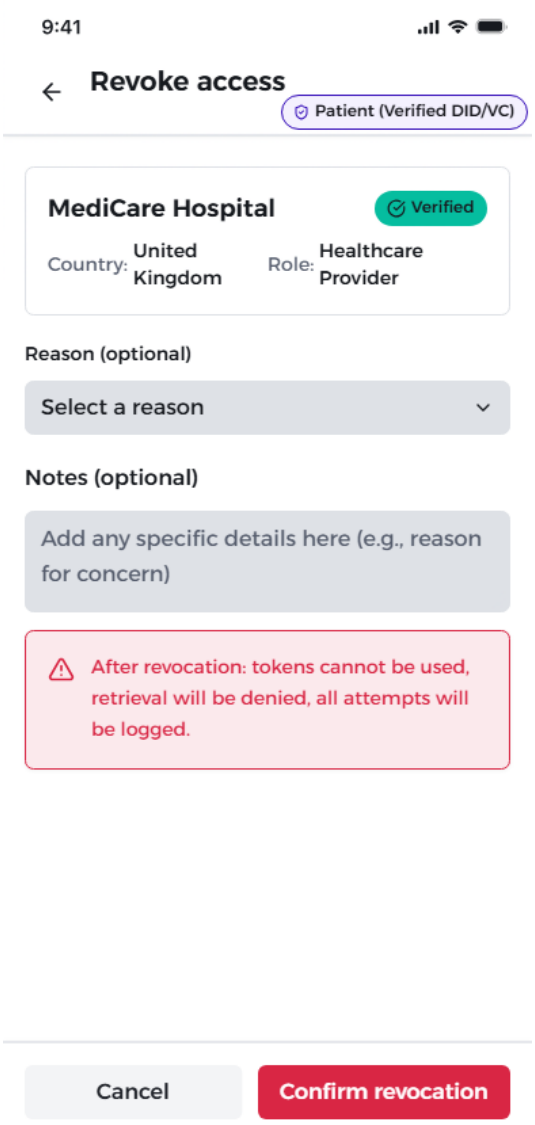


Figure 14 - Revocation confirmation with reason code and effect summary.

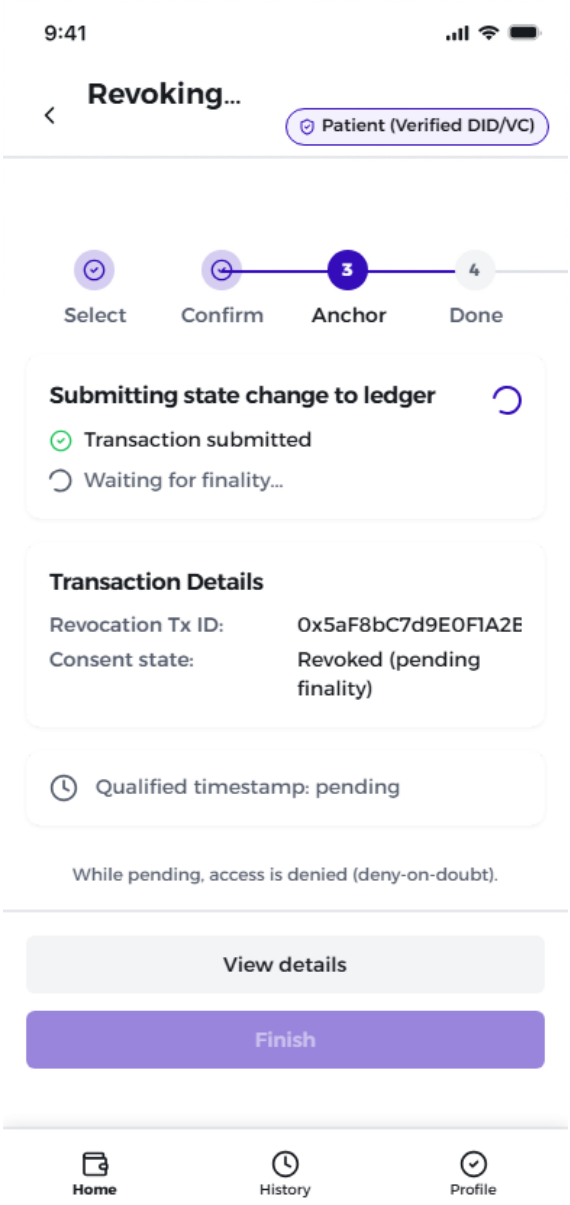


Figure 15 - Revocation anchoring progress with ledger confirmation and time reference.

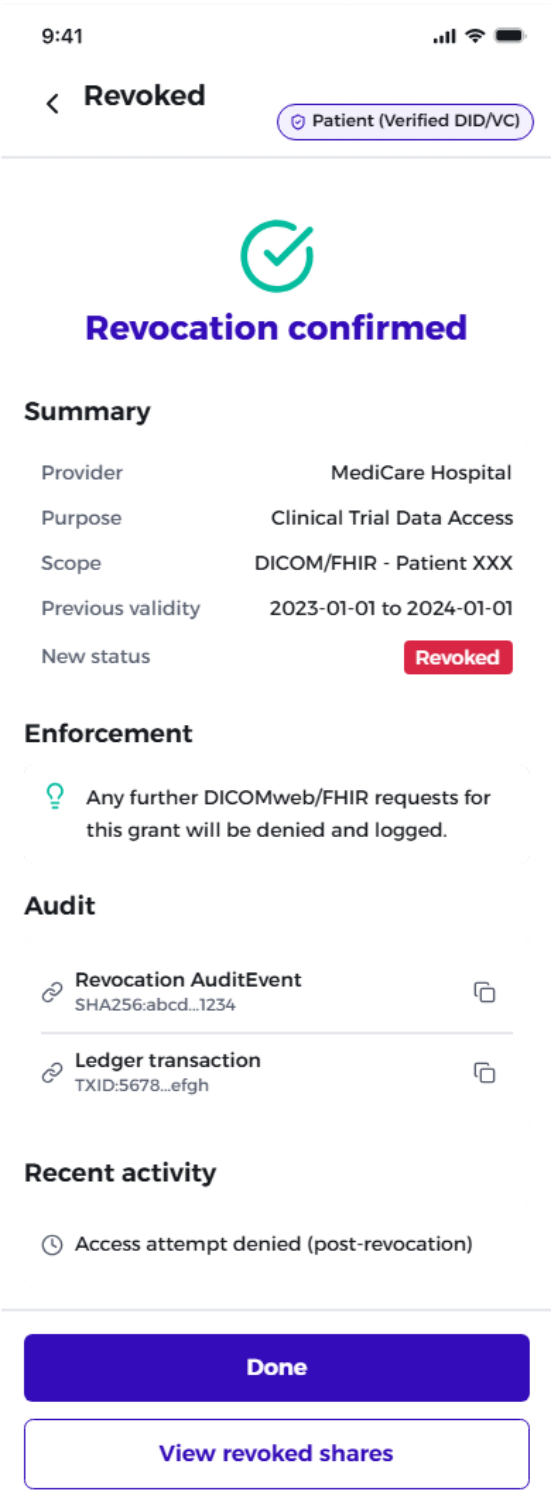


Figure 16 - Revocation success summary with audit link and enforcement note.

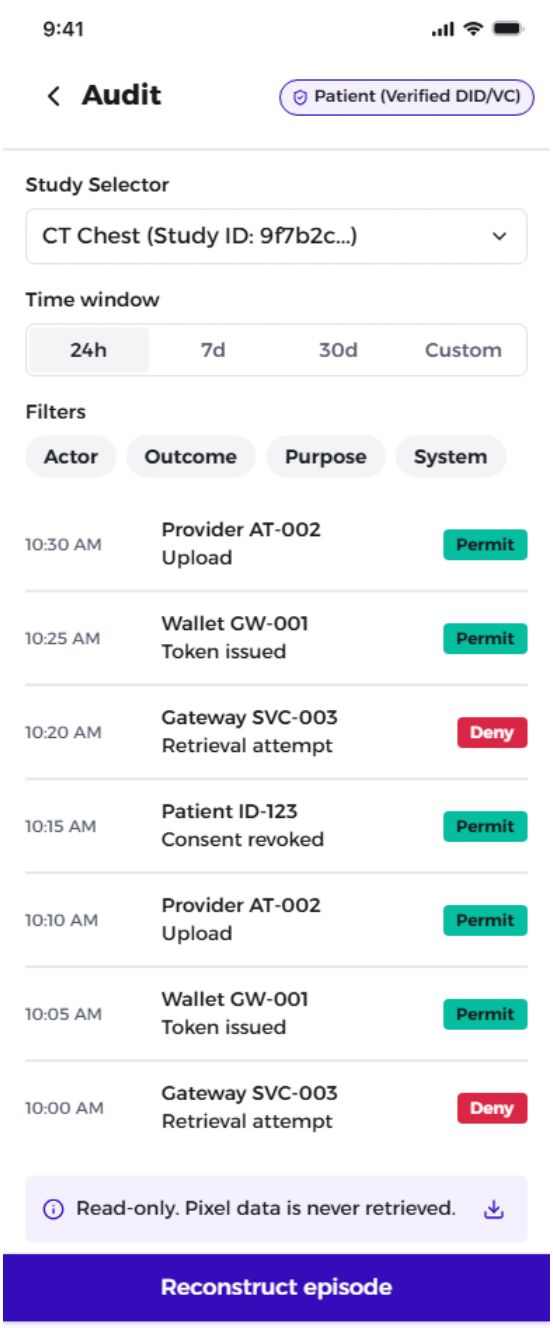


Figure 17 - Audit timeline with study selector, time window and filter chips.

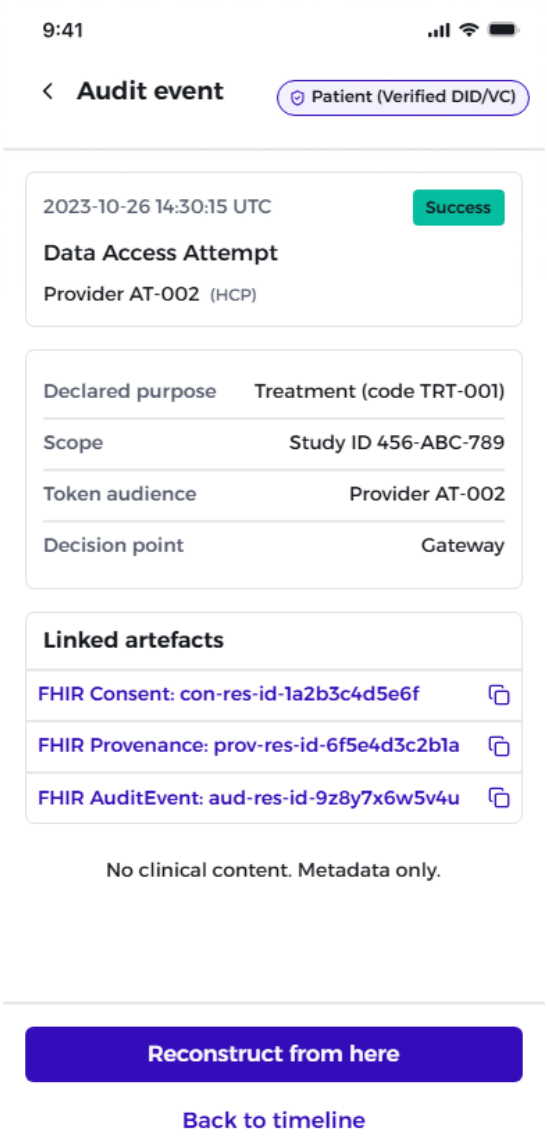


Figure 18 - Event detail panel with links to Consent and Provenance.

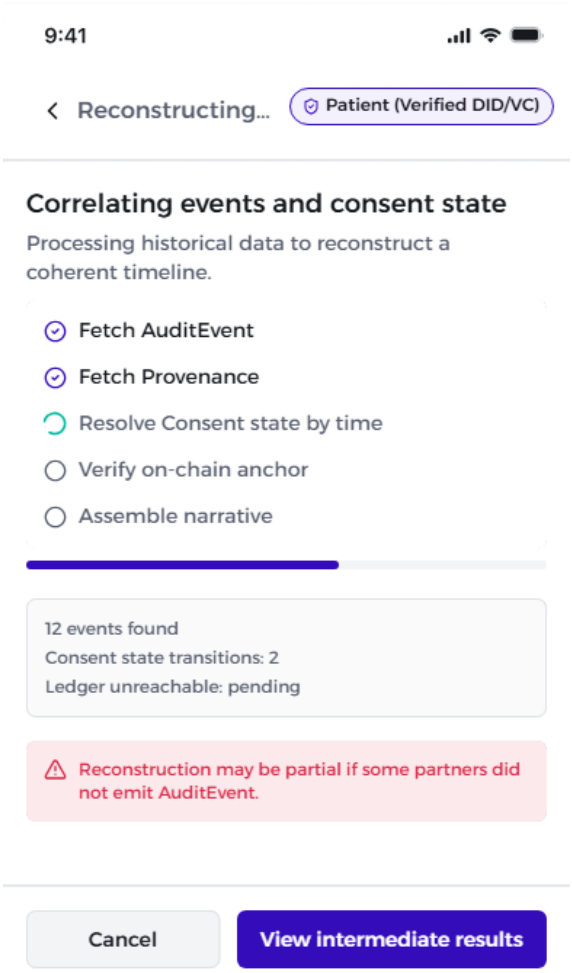


Figure 19 - Reconstruction progress with correlation to consent state and on-chain anchor check.

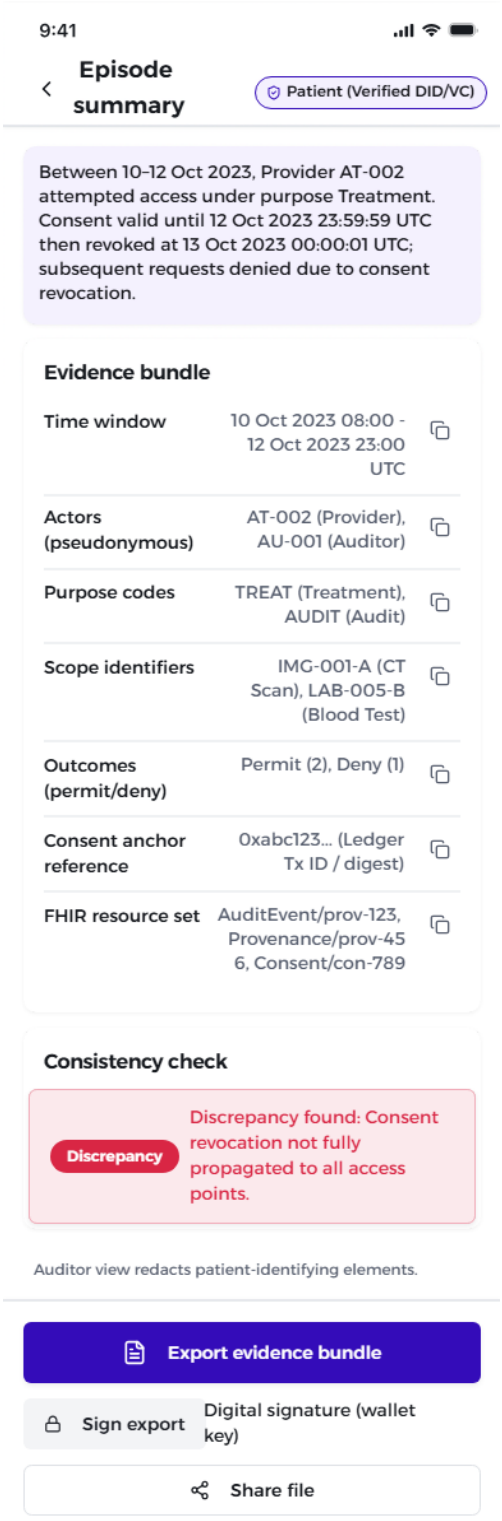


Figure 20 - Consolidated narrative and exportable evidence-bundle summary.