BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

ORIGINAL RESEARCH

A Blockchain-Based Architecture for Dynamic and Auditable Patient Consent in Secondary Use of Health Data

Sudip Phuyal, MSc[1], Manila Bhandari, MSc[1], Rabindra Bista, PhD[2] and João Carlos Ferreira, PhD[3,4]

[1]Information Sciences, Technology and Architecture Research Center (ISTAR-ISCTE), University Institute of Lisbon, Lisbon, Portugal; [2]Department of Computer Science and Engineering, Kathmandu University, Kathmandu, Nepal; [3]Department of Logistics, Molde University College, Molde, Norway; [4]Inov Inesc, 1000-029 Lisbon, Portugal

DOI: https://doi.org/10.30953/bhty.v9.491

Corresponding Author: João Carlos Ferreira, Email: joam@himolde.no

Keywords: blockchain, consent management, digital health, health data, interoperability, reuse, patient empowerment

Abstract

Background: The secondary use of patient health data is critical for advancing clinical research, public health, and digital health innovation. However, traditional consent mechanisms are often static, complex, and insufficiently transparent, limiting patient control and trust. In response to regulatory requirements introduced by the General Data Protection Regulation (GDPR) and the European Health Data Space (EHDS), this article paper aims to design a secure, transparent, and revocable blockchain-based architecture for managing patient consent for the secondary use of health data, aligned with European legal frameworks and interoperability standards.
Methods: A multilayered consent management architecture was designed by integrating blockchain smart contracts, decentralized identifiers, verifiable credentials, and Health Level Seven—Fast Healthcare Interoperability Resources. The system incorporates a patient-controlled digital wallet, off-chain health data storage, and on-chain enforcement of consent policies through smart contracts. Regulatory and technical requirements were systematically derived from GDPR and European Health EHDS provisions. The study follows a design science research methodology and includes threat modeling and a theoretical performance and scalability analysis. The design is guided by four core objectives: dynamic consent management, auditable governance, interoperability with healthcare standards, and compliance-by-design with European regulatory frameworks.
Results: The proposed architecture enables secure creation, delegation, and revocation of patient consent through immutable blockchain-based logging and Fast Healthcare Interoperability Resources-compliant data exchange. Consent records are tamper-evident, while sensitive health data remain off-chain, ensuring data minimization and privacy protection. Consent attributes such as purpose limitation, duration, and data scope are explicitly modeled to comply with GDPR and EHDS requirements. Theoretical evaluation indicates that the architecture can scale to large healthcare data ecosystems when deployed on Ethereum-compatible blockchains combined with external storage solutions.
Conclusions: This study presents a modular, standards-based consent management framework that enhances patient autonomy, supports regulatory compliance, and strengthens governance for the secondary use of health data. By combining blockchain, digital identity, and healthcare interoperability standards, the architecture addresses key legal and technical challenges of dynamic consent. Future work will focus on developing a user-centered prototype and conducting empirical validation in real-world secondary-use health data ecosystems.

Plain Language Summary

The secondary use of patient health data plays a vital role in advancing clinical research, public health, and digital health innovation; however, prevailing consent mechanisms are often static, opaque, and difficult for patients to control. In response to regulatory requirements introduced by the General Data Protection Regulation (GDPR) and the European Health Data Space (EHDS), this paper proposes a secure, transparent, and revocable blockchain-based architecture for managing patient consent for the secondary use of health data. The proposed solution adopts a multilayered design integrating blockchain smart contracts, decentralized identifiers (DIDs), verifiable credentials (VCs), and Health Level Seven—Fast Healthcare Interoperability Resources. It combines patient-controlled digital wallets, off-chain health data storage, and on-chain enforcement of consent policies to ensure data minimization and privacy protection. Regulatory and technical requirements are systematically derived from GDPR and EHDS provisions, and the study follows a Design Science Research methodology supported by threat modeling and theoretical performance and scalability analysis. The architecture enables fine-grained consent creation, delegation, and revocation, with consent attributes such as purpose limitation, duration, and data scope explicitly modeled to support legal compliance. Immutable blockchain-based logging ensures auditability and trust while avoiding on-chain storage of sensitive health data. Theoretical evaluation indicates that the architecture can scale to large healthcare ecosystems when deployed on Ethereum-compatible blockchains with external storage solutions. The proposed framework enhances patient autonomy, strengthens governance for secondary health data use, and provides a standards-based foundation for future implementation and real-world validation.

Received: February 4, 2026; Accepted: April 15, 2026; Published: April 28, 2026

The secondary use of health data, defined as the reuse of clinical, administrative, or patient-generated data beyond direct care, has become central to contemporary digital health ecosystems. Such reuse underpins biomedical research, public health surveillance, health system planning, and the development of data-driven innovations, including artificial intelligence-enabled clinical decision support systems. As the volume and diversity of health data continue to expand through electronic health records (EHRs), genomics, mobile health applications, and wearable devices, the potential societal value of secondary data use has also grown significantly. However, realizing these benefits requires robust governance mechanisms that respect individual autonomy and protect privacy.

At the same time, this rising trend has increased ethical, legal, and governance challenges related to patient autonomy, trust, and data protection in large-scale digital health ecosystems. One of the major challenges in secondary health data reuse is the management of individual patient consent. Conventional consent mechanisms are typically static, paper-based, or embedded within centralized digital platforms that leave patients with limited control and visibility. Once consent is granted, patients often struggle to understand how their data are reused, who has access to them, or how consent can be withdrawn at a later stage if they so choose. This lack of ongoing control and transparency can reduce patient trust and willingness to participate in research and other initiatives that rely on the secondary use of health data,[1] while dynamic consent approaches have been suggested to address many of these gaps.[2] Dynamic consent enables participants to continuously review and update their preferences, potentially improving engagement and trust.

Within the European Union (EU), these challenges are being addressed through the regulatory frameworks that place patient rights and accountability at the core of data governance. The GDP establishes consent as a lawful basis for processing personal data and requires consent to be informed, specific, and revocable at any time. More recently, the European Health Data Space (EHDS) regulation has introduced additional criteria for the secondary use of health data, including traceable access, purpose limitation, and the use of digital tools to support patient-managed consent. The EHDS also aims to harmonize secondary use governance across Member States and provide individuals better control over their data,[3] including enforceable rights such as opt-out mechanisms.[4,5] While consent is a central mechanism for many secondary-use scenarios, European data protection frameworks also permit secondary processing under alternative lawful bases, such as tasks carried out in the public interest or processing mandated by law under General Data Protection Regulation (GDPR) and the EHDS. Accordingly, the proposed architecture is consent-first but extensible to opt-out and lawful-basis tagging workflows, allowing authorization decisions to be evaluated and audited regardless of whether consent or an alternative legal basis applies. This approach preserves traceability, accountability, and transparency of secondary-use access decisions across heterogeneous regulatory contexts.

However, empirical assessments at the EU level indicate that, despite the harmonizing intent of the GDPR, its national implementations are highly fragmented, particularly regarding secondary use of health data. A comprehensive European Commission study examining Member State rules found substantial variation in legal interpretation, governance structures, and operational practices, which collectively hinder cross-border data sharing for research, public health, and system management.[6] The study further highlights that patients do not always find it easy to exercise their GDPR rights in practice and that inconsistent national rules undermine trust, interoperability, and accountability. These findings underscore the need for technically enforced, standards-based consent and audit mechanisms capable of operating consistently across jurisdictions, as envisioned by the EHDS. Together, these developments signal a shift toward dynamic, auditable, and patient-centric consent models as a prerequisite for trustworthy secondary health data sharing across Europe.

Despite this regulatory progress, existing digital consent solutions often fail to operationalize these principles effectively in practice.[7] Many platforms rely on centralized architectures that concentrate control within data-holding institutions or third-party service providers, thereby limiting patient sovereignty and introducing single points of failure. Other approaches lack interoperability with established health information standards, making integration with EHR systems and cross-border infrastructures difficult. As a result, a substantial gap remains between regulatory expectations for dynamic and transparent consent and the technical capabilities of current health data ecosystems to support large-scale secondary use.

Distributed ledger technologies, commonly referred to as blockchain, have emerged as potential enablers of transparent and tamper-evident consent management. Blockchain-based systems provide immutable and shared records of transactions that can support verifiable audit trails and programmable enforcement of consent rules.[8,9] When combined with decentralized identity technologies such as decentralized identifiers (DIDs) and verifiable credentials (VCs), these systems offer the possibility of patient-controlled authentication and authorization without reliance on a single central authority.[10] However, most blockchain-based consent proposals remain conceptual or limited to proof-of-concept implementations and frequently lack alignment with healthcare interoperability standards or the specific legal requirements governing secondary health data use in Europe.[11–13]

Limited attention has been given to integrating blockchain-enabled consent mechanisms with **Health Level Seven (**HL7) Fast Healthcare Interoperability Resources (FHIR), which has become the de facto standard for health data exchange. Without such integration, consent systems risk becoming disconnected from real-world clinical and research workflows.[14] Recent research highlights the importance of combining consent governance with interoperability standards to facilitate real-world adoption.[15] Moreover, few existing approaches explicitly map technical design choices to GDPR and EHDS requirements, leaving uncertainty regarding their suitability for deployment in regulated health data environments such as national health data spaces.

In this context, this paper presents a patient-centric architectural model as its primary outcome, designed to enable dynamic and auditable consent management for the secondary use of health data. The proposed architecture combines

Citation: Blockchain in Healthcare Today 2026, **9**: 491 - https://doi.org/10.30953/bhty.v9.491

blockchain-based smart contracts, decentralized identity wallets, VCs, and HL7 FHIR consent resources to support the full consent lifecycle, including issuance, monitoring, revocation, and audit. Personal health data remain stored off-chain within trusted institutional repositories, while cryptographic references and consent state changes are recorded on-chain to ensure integrity, transparency, and regulatory accountability without exposing sensitive data.

The contribution of this work, embodied in the proposed architecture, is threefold. First, it conceptualizes consent as a continuous, patient-managed lifecycle rather than a one-time authorization event, in line with ethical considerations and European regulatory requirements. Second, it demonstrates how established digital health standards can be combined with decentralized identity technologies to achieve interoperability and privacy-by-design in secondary data governance. Third, it provides a compliance-oriented architectural blueprint that can inform future implementations and policy discussions related to the EHDS.

By positioning blockchain as an enabling trust and governance layer rather than a data storage solution, this study contributes to the responsible design of patient-centered digital health infrastructures. The proposed architecture supports trustworthy secondary health data use by strengthening patient autonomy, transparency, and confidence in data-driven health innovation while remaining compatible with existing health information systems.

Unlike prior blockchain-based consent proposals, the proposed architecture integrates dynamic consent lifecycle management, HL7 FHIR-based consent representation, decentralized identity through DIDs and VCs, and explicit GDPR/EHDS compliance mapping within a single governance-oriented framework for secondary health data use.

Related Works

The management of patient consent for the secondary use of health data has been extensively discussed in the digital health and biomedical research literature, particularly in relation to ethical governance, patient autonomy, and trust.[16,17] Early consent models were largely designed for single-purpose clinical or research studies and relied on static, paper-based agreements or one-time digital authorizations. While these approaches facilitated data access, they provided limited support for ongoing patient engagement, post-authorization transparency, or the ability to modify or withdraw consent once data were shared. As health data reuse has expanded across institutional and national boundaries, these limitations have become increasingly evident in large-scale digital health ecosystems.

In response, several digital consent paradigms have been proposed to enhance patient involvement and flexibility. Broad consent and meta-consent models allow individuals to authorize categories of future research or to define how they wish to be asked for consent across different contexts. Dynamic consent platforms extend these ideas by enabling continuous communication between patients and data users through digital interfaces. Although these approaches represent important conceptual advances, most implementations rely on centralized infrastructures and institutional trust. As a result, they often lack verifiable auditability, real-time enforcement of consent withdrawal, and seamless interoperability with EHR systems and secondary data platforms. Dynamic consent has also been proposed in blockchain-enabled contexts to improve patient control and the transparency of consent lifecycle events; for example, protocols for integrative reviews are being developed to critically assess blockchain-based dynamic consent implementations in health data sharing and research contexts[2] and to identify design patterns for patient-centric governance.

The introduction of the GDPR has further shaped the consent landscape by establishing explicit legal requirements for informed, purpose-bound, and revocable consent. Recent studies have explored GDPR-compliant consent management solutions, emphasizing accountability and transparency. The EHDS builds on these principles by introducing additional obligations for traceable access, digital consent tools, and cross-border governance of secondary health data use. Despite this regulatory momentum, many proposed solutions focus primarily on legal interpretation or organizational processes rather than on operational system architectures capable of enforcing these requirements in distributed digital health environments at scale.

Blockchain technology has been proposed as a potential mechanism to improve transparency and accountability in health data sharing.[9,18] Blockchain-enabled systems provide immutable and shared records of transactions that can support verifiable audit trails and programmable enforcement of consent rules. Recent frameworks for blockchain-enabled consent management outline decentralized consent enforcement architectures emphasizing smart contract-based enforcement, auditability, and regulatory compliance, with a focus on patient privacy preferences and granular control.[19] This direction is also reflected in prior work on blockchain-based smart-contract enforcement of human-subject governance and pilot implementations of blockchain-supported informed consent workflows in clinical research.[9,18] However, many blockchain-based consent solutions are still conceptual or lack integration with established health interoperability standards such as HL7 FHIR, limiting their practical utility in operational EHR workflows. Early systems such as MedRec demonstrated the feasibility of using blockchain for access logging, while later initiatives attempted to integrate blockchain with health data exchange standards.[16] However, many blockchain-based consent solutions focus on primary data access or treat consent as a static permission rather than a dynamic lifecycle. Furthermore, several approaches store excessive metadata on-chain or lack explicit alignment with GDPR principles such as data minimization and the right to withdraw consent, raising concerns about privacy and regulatory suitability in real-world healthcare deployments.

More recent explorations suggest integrating blockchain with standardized health IT frameworks to enhance consent interoperability; for example, work on blockchain-enabled consent models in FHIR-compliant platforms has been proposed to bridge decentralized ledgers with existing clinical data exchange standards.[13,20] While promising, such approaches often remain at the theoretical or pilot stage, and empirical evidence of large-scale deployment in regulated healthcare environments is still limited, particularly for secondary-use governance across institutional and national boundaries.

To summarize the strengths and limitations of existing approaches, Table 1 compares centralized dynamic-consent

Table 1. Comparison of consent management approaches for secondary use of health data.

Approach	Patient control & revocation	Auditability & enforcement	Interoperability & standards alignment
Centralized dynamic-consent platforms	High patient interaction; revocation often policy-driven and not technically enforced across all downstream copies	Audit trails depend on the platform operator; limited third-party verifiability	Varies; often limited or proprietary integrations
Blockchain consent (static permission)	Consent captured at one point in time; revocation may not invalidate future access cleanly	Strong immutability for logs; enforcement sometimes limited to access logging rather than consent logic	Often weak linkage to HL7 FHIR or operational EHR workflows
Blockchain + smart contracts (consent logic)	Improved technical revocation; risk of storing excessive metadata on-chain	Programmable checks and logs; privacy depends on on-chain data minimization	Usually, limited identity and standards integration
This paper (Blockchain + DID/VC + FHIR, off-chain data)	Dynamic lifecycle with revocation; patient wallet mediates grant/withdrawal	Tamper-evident consent proofs and state transitions; enforcement via consent-state validation	Explicit HL7 FHIR representation and DID/VC-based authorization; designed for EU secondary-use governance

DID/VC: Decentralized Identifiers/Verifiable Credentials; EHR: electronic health record; EU: European Union; HL7 FHIR: Health Level Seven—Fast Healthcare Interoperability Resources.

platforms, blockchain-based static consent models, and blockchain systems with smart contract–based consent logic against the proposed architecture of this study. The comparison evaluates each approach across key architectural dimensions including patient control and revocation, auditability and enforcement, interoperability with HL7 FHIR standards, and alignment with European regulatory frameworks governing secondary health data use.

Taken together, existing approaches reveal a persistent gap in the literature. Traditional and dynamic consent platforms offer patient engagement but lack decentralized governance and verifiable auditability, while many blockchain-based solutions improve transparency but frequently overlook interoperability and regulatory alignment. Few studies combine patient-centric identity management, standards-based consent representation, and compliance with European regulatory frameworks within a single architecture. This study addresses this gap by proposing an integrated, patient-centric consent management architecture that supports dynamic consent, auditability, and interoperability for the secondary use of health data under GDPR and EHDS within a unified governance framework.

Contributions of this Article

This article contributes to the field of digital health data governance by proposing a patient-centered, standards-based architecture for managing consent in the secondary use of health data. The key contributions are as follows:

Patient-Centric Model for Dynamic Consent in Secondary Health Data Use

The study conceptualizes patient consent as a continuous and revocable lifecycle rather than a one-time authorization event. By enabling patients to grant, monitor, and withdraw consent over time, the proposed architecture strengthens patient autonomy and supports ethical participation in research and secondary data-sharing initiatives across distributed healthcare ecosystems.

An Interoperable Consent Architecture Aligned with Healthcare Standards

The architecture integrates decentralized identity technologies, digital wallets, and HL7 FHIR to ensure compatibility with existing EHR systems and research infrastructures. This standards-based approach facilitates real-world integration across heterogeneous health data environments and supports cross-institutional and cross-border data reuse without disrupting legacy systems.

Transparent and Auditable Consent Governance Mechanism

By leveraging blockchain-based logging as a trust and audit layer, the proposed system provides tamper-evident records of consent issuance, modification, and revocation. This design enables verifiable accountability for data access decisions while avoiding the storage of personal health data on-chain, thereby supporting regulatory oversight without compromising patient privacy or violating data minimization principles.

Privacy-Preserving, Compliance-by-Design Approach

The architecture explicitly aligns technical design choices with key requirements of the GDPR and the EHDS, including consent revocability, data minimization, and traceable access. This regulatory mapping offers practical guidance for implementing legally compliant consent mechanisms in European digital health ecosystems and for informing governance models in emerging health data spaces.

Conceptual Blueprint for Responsible Secondary Data Governance

Rather than presenting a narrowly scoped technical solution, this study provides a modular architectural blueprint that can inform future implementations, pilot deployments, and policy discussions. The proposed model is intended to support trustworthy secondary health data use while balancing innovation, patient rights, and regulatory accountability in large-scale, federated digital health environments.

Methods

Study Design

This study adopts a design-oriented qualitative methodology to develop and conceptually evaluate a patient-centered architecture for managing consent in the secondary use of health data. The work follows principles of design science research, in which a novel socio-technical artifact is created to address a clearly defined digital health governance challenge: enabling dynamic, auditable, and legally compliant patient consent under European health data regulations for secondary data use.

Citation: Blockchain in Healthcare Today 2026, **9**: 491 - https://doi.org/10.30953/bhty.v9.491

As the study does not involve human participants, real-world patient data, or system deployment, no empirical experimentation or user evaluation was conducted. Instead, the methodological focus is on architectural design, standards-based modeling, and regulatory alignment, which are appropriate for early-stage digital health infrastructure research intended to inform future implementation, evaluation, and policy development in regulated healthcare environments.

Design Science Research Framing

Following Design Science Research principles,[21] the artifact produced by this study is the proposed consent-management architecture, including its workflow models (consent lifecycle), standards mappings (FHIR, DID/VC), and the regulatory traceability mapping to GDPR and EHDS requirements. The artifact is intended as an implementable blueprint rather than a deployed system, suitable for guiding prototyping and pilot deployments in regulated European health-data environments and secondary-use governance contexts.

Consistent with DSR evaluation guidance for early-stage artifacts, the design is assessed through: (1) internal coherence of components and trust boundaries, (2) standards and regulatory alignment, and (3) qualitative feasibility of integration into existing clinical and secondary-use data infrastructures without disrupting established operational workflows.

In line with established DSR methodologies, the study emphasizes the relevance of the problem context, the rigor of standards and regulatory grounding, and the utility of the artifact as a foundation for subsequent instantiation and evaluation.

Design Objectives and Requirements

The architecture was designed to address functional, ethical, and regulatory requirements identified through a review of existing consent models and European data protection frameworks.

To ensure clarity and traceability, the design objectives are explicitly defined as follows:

1. Dynamic and Revocable Consent: Enable patients to grant, monitor, and withdraw consent continuously across the data lifecycle.

2. Transparent and Auditable Governance: Provide tamper-evident logging and verifiable auditability of consent decisions and data access events.

3. Interoperability and Standards Alignment: Ensure compatibility with HL7 FHIR and integration with heterogeneous health data systems.

4. Privacy and Compliance by Design: Enforce data minimization and align system behavior with GDPR and EHDS requirements.

Core design objectives included enabling patients to dynamically grant and withdraw consent, supporting transparent and traceable authorization for secondary data use, preserving privacy through data minimization, and ensuring interoperability with existing healthcare information systems across organizational and national boundaries.

Regulatory requirements were derived primarily from the GDPR and the EHDS. Emphasis was placed on consent revocability, accountability, purpose limitation, and traceable access as enforceable system capabilities rather than solely policy obligations. Technical design requirements focused on modularity and standards alignment to support heterogeneous healthcare environments and cross-border data sharing within federated secondary-use infrastructures.

Together, these objectives guided the architecture toward a compliance-by-design approach in which legal, ethical, and technical requirements are embedded directly into system components and workflows, rather than addressed through external governance mechanisms alone.

Architecture Modeling Approach

The system was modeled using a workflow- and actor-oriented architectural approach that reflects how consent decisions are created, enforced, and audited in real-world secondary data use scenarios. Rather than focusing solely on technical components, the modeling process emphasized interactions among patients, data requesters, consent governance services, health data repositories, and regulatory oversight actors to capture socio-technical dependencies and trust boundaries.

System context and container-level architectural views were developed to capture trust boundaries, data flows, and governance responsibilities. These architectural views constitute the primary design artifacts of the study and are presented in the Results section using the C4 model notation to ensure clarity and stakeholder accessibility.

This multilevel modeling approach supports reasoning about both high-level governance interactions and lower-level system responsibilities, enabling systematic analysis of security, interoperability, and compliance implications across the consent lifecycle.

Standards and Technology Selection

Interoperability and governance considerations guided the selection of standards and enabling technologies used in the architecture. HL7 FHIR was selected to represent consent metadata and to link authorization decisions with clinical and research data systems because of its widespread adoption and support for standardized consent representation. DIDs and VCs were incorporated to support patient-controlled identity and cryptographically verifiable consent authorization in decentralized and cross-organizational environments.[10]

Blockchain technology was selected as an enabling trust and audit layer, providing tamper-evident logging of consent-related events without storing personal health data on-chain. The architecture is designed to be compatible with Ethereum-based blockchain infrastructures and can be deployed on either public or permissioned networks depending on governance requirements. Public blockchain deployments may provide strong transparency and decentralized verification, while permissioned networks may offer greater control over participation and operational governance within healthcare ecosystems. To balance transparency with operational scalability, the architecture may also leverage Layer-2 networks such as Polygon or Optimism to reduce transaction costs while maintaining cryptographic anchoring to a secure base layer.

This separation supports privacy-by-design principles and aligns with regulatory requirements for data minimization under the GDPR and EHDS. Table 2 summarizes the primary standards and frameworks integrated into the proposed architecture and their roles within the consent governance workflow.

Together, these standards and technologies enable a modular architecture that can interoperate with existing health information infrastructures while introducing decentralized governance capabilities required for dynamic, auditable secondary-use consent management.

Regulatory Mapping and Compliance-by-Design

To ensure legal robustness, system functions were systematically mapped to relevant provisions of the GDPR and the EHDS. This compliance-by-design approach ensured that regulatory requirements, such as the right to withdraw consent, traceable access, and accountability, were embedded directly into architectural design decisions rather than addressed through external policies or post hoc controls[22] or organizational procedures alone.

The regulatory mapping informed both functional requirements and architectural constraints and served as a primary mechanism for validating alignment with European health data governance frameworks. The resulting compliance implications are presented as part of the design outcomes in the Results section to demonstrate how legal principles are operationalized as system capabilities.

By translating abstract regulatory obligations into concrete architectural mechanisms, the proposed approach supports demonstrable accountability and facilitates regulatory oversight in distributed secondary-use data ecosystems.

Conceptual Evaluation Framework

Given the absence of empirical deployment, the proposed architecture was evaluated conceptually across three analytical dimensions: security, scalability, and regulatory compliance. Security analysis focused on the integrity and non-repudiation of consent records, scalability analysis examined the feasibility of supporting large-scale secondary data ecosystems, and compliance analysis assessed alignment with GDPR and EHDS principles as operational system properties.

This conceptual evaluation provides assurance that the proposed architecture is coherent, feasible, and suitable as a foundation for future prototype development, user-centered evaluation, and real-world pilot deployment in European digital health contexts where secondary-use governance and cross-border data sharing are critical.

Although qualitative in nature, this evaluation framework aligns with design science guidance for early-stage artifacts by emphasizing internal validity, relevance to practice, and readiness for subsequent instantiation and empirical assessment.

Table 2. Standards and frameworks integrated in the proposed architecture.

Standard or framework	Role in the architecture
HL7 FHIR	Standardized representation of consent metadata and linkage to health data systems
Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs)	Patient-controlled identity and verifiable authorization
ISO 27789	Principles for traceable and auditable health record access
GDPR and EHDS	Legal framework governing consent, accountability, and secondary data use

GDPR: General Data Protection Regulation; EHDS: European Health Data Space; DIDs: Decentralized Identifiers; HL7 FHIR: Health Level Seven—Fast Healthcare Interoperability Resources; VCs: Verifiable Credentials.

Evaluation Criteria and Assumptions

Given the absence of empirical deployment, the proposed architecture was evaluated conceptually across three analytical dimensions: security, scalability, and regulatory compliance. Security analysis focused on the integrity and non-repudiation of consent-state changes, scalability analysis examined the feasibility of supporting large-scale secondary data ecosystems, and compliance analysis assessed alignment with GDPR and EHDS principles as operational system properties.

This conceptual evaluation provides assurance that the proposed architecture is coherent, feasible, and suitable as a foundation for future prototype development, user-centered evaluation, and real-world pilot deployment in European digital health contexts where secondary-use governance and cross-border data sharing are critical.

Although qualitative in nature, this evaluation framework aligns with design science guidance for early-stage artifacts by emphasizing internal validity, relevance to practice, and readiness for subsequent instantiation and empirical assessment.

Security

Security evaluation considers the integrity of consent-state changes, non-repudiation of consent actions, and resistance to unauthorized consent manipulation, such as forged requests or replay of expired consents. Blockchain-based append-only logging ensures tamper-evident recording of consent issuance, modification, and revocation events, while cryptographic signatures and decentralized identity mechanisms support authentication and accountability of participating actors. Availability and denial-of-service risks are acknowledged but treated as operational concerns mitigated through standard infrastructure protections rather than as primary design objectives of the ledger-based audit layer.

To provide a structured threat-oriented view, Table 4 summarizes key security threats using a condensed STRIDE-style (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) (STRIDE)-style classification and maps them to architectural mitigations and residual risks. This analysis highlights that the architecture primarily addresses integrity, authorization, and accountability threats at the consent-governance layer, while recognizing that certain risks remain dependent on endpoint security and organizational controls.

This threat summary does not aim to provide exhaustive security assurance but rather to demonstrate that common threat classes are explicitly considered and addressed at the architectural level, consistent with the scope of a conceptual design evaluation.

Scalability

Scalability feasibility is evaluated in terms of expected consent-event volume (creation, update, revocation, and delegation) relative to blockchain write capacity, assuming that only

Citation: Blockchain in Healthcare Today 2026, **9**: 491 - https://doi.org/10.30953/bhty.v9.491

Table 3. Design science evidence matrix.

Requirement/Objective	Architectural mechanism	Evidence type
Dynamic, revocable consent	Consent lifecycle + wallet-mediated decisions	Workflow artifact + consistency argument
Prevent future unauthorized access	Gateway authorization checks	Logical enforcement argument
Auditability	Immutable consent and access logs	Threat analysis + non-repudiation
Data minimization	Off-chain PHI, on-chain hashes	GDPR compliance mapping
Interoperability	HL7 FHIR Consent usage	Standards conformance argument
Identity assurance	DID/VC-based authorization	Trust framework assumptions
Regulatory compliance	GDPR/EHDS mapping	Compliance-by-design table
Scalability	Minimal on-chain writes	Capacity and feasibility argument

GDPR/EHDS: General Data Protection/European Health Data Space; HL7 FHIR: Health Level Seven—Fast Healthcare Interoperability Resources; PHI: Personally Identifiable Health Information; VC: Verifiable Credentials.

Table 4. STRIDE-style threat summary.

Asset	Threat	Mitigation	Residual risk
Consent state	Tampering	Append-only ledger, cryptographic signatures	Key compromise
User identity	Spoofing/repudiation	DID/VC verification	Wallet misuse
Consent metadata	Information disclosure	Off-chain storage of metadata	Traffic analysis
Availability	DoS	Rate limiting, batching	Infrastructure-level
Authorization logic	Privilege escalation	Gateway enforcement	Insider misuse

DID/VC: Decentralized Identifier/Verifiable Credentials; DoS: denial-of-service; STRIDE-style: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege.

minimal consent proofs and state pointers are stored on-chain and that health data and rich metadata remain off-chain. This assumption is consistent with data-minimization principles under GDPR and avoids on-chain accumulation of personal data that could hinder long-term scalability.

On-chain writes are limited to consent lifecycle events, with only compact cryptographic proofs recorded on the ledger. Through batching strategies or periodic anchoring of Merkle roots representing multiple consent events, ledger growth remains proportional to governance activity rather than to underlying data volume. This design ensures that the architecture can scale to high-volume secondary-use environments without introducing prohibitive storage or throughput constraints at the blockchain layer.

To provide indicative operational context, typical consent lifecycle events require only minimal on-chain operations, such as recording a consent state hash or anchoring a Merkle root representing multiple consent updates. On Ethereum-compatible Layer-2 networks, these operations typically incur relatively low transaction costs. For example, a simple hash anchoring transaction may consume approximately 40,000 to 60,000 gas units. On Layer-2 networks such as Polygon or Optimism, this corresponds to an approximate cost of less than USD $0.01–$0.05 per transaction under typical network conditions.

Consent creation and revocation events, therefore, remain economically feasible even at large scale. Additionally, batching strategies can aggregate multiple consent updates into a single Merkle root anchoring transaction, significantly reducing the number of on-chain operations required. Under this approach, a single blockchain transaction can represent dozens or hundreds of consent lifecycle events while maintaining verifiable integrity guarantees.

Because authorization checks occur primarily at institutional gateways using off-chain consent metadata stored in FHIR repositories, the blockchain layer serves primarily as an integrity and audit anchor rather than a high-throughput processing system. This design minimizes blockchain load while preserving tamper-evident governance capabilities.

Compliance

Compliance alignment is evaluated by mapping each consent lifecycle capability (request, grant, enforce, revoke, and audit) to specific GDPR and EHDS requirements and by ensuring that the architecture supports demonstrable accountability without requiring on-chain storage of personal health data or irreversible consent metadata. Consent revocability, purpose limitation, traceable access, and accountability are thus treated as enforceable system properties rather than as policy-only obligations.

These criteria and assumptions define the scope and limits of the conceptual evaluation and provide a transparent basis for interpreting the feasibility and governance implications of the proposed architecture prior to empirical validation.

Results

Overview of Design Outcomes

Results are reported as design artifacts, including architectural models, standards mappings, and conceptual evaluation tables, rather than as empirical performance or deployment outcomes. The primary outcome of this study is a patient-centered, standards-based architecture for managing consent in the secondary use of health data. As this work is conceptual and design-oriented, the Results section presents the architectural artifacts, consent governance workflows, and interoperability and compliance outcomes produced through the design process, rather than empirical performance measurements or implementation results.

The resulting architecture operationalizes dynamic, revocable consent as a continuous lifecycle, integrates established health data and identity standards, and embeds regulatory compliance with European data protection frameworks. Figures 1 and 2 illustrate the system context and internal structure of the proposed solution using container- and context-level architectural views.

Together, these design outcomes demonstrate how a modular, governance-oriented architecture can support patient-driven consent management while remaining interoperable with existing health information infrastructures and compliant with European regulatory requirements for secondary data use.

System Context and Stakeholder Interactions

Figure 1 presents the system context view of the proposed consent management architecture, highlighting the primary stakeholders involved in secondary health data use and their interactions. The architecture centers on five key roles: patients, data requesters, consent governance services, health data repositories, and regulatory or oversight authorities that collectively shape secondary-use data governance.

Patients interact with the system through a digital wallet that enables them to receive secondary-use requests, review consent parameters, and grant or revoke authorization. Data requesters such as researchers, public health bodies, or analytics providers submit structured requests specifying the purpose, scope, and duration of data use. Consent governance services validate requests, record consent states, and enforce authorization decisions. Health data repositories retain personal health data off-chain and release data only when valid consent is confirmed. Oversight authorities can verify consent-related events and access decisions through audit mechanisms without accessing personal health data.

This system context demonstrates how patient-driven consent decisions can be enforced and verified across distributed organizational environments while maintaining clear accountability boundaries and supporting traceable governance of secondary health data access.

Architectural Structure and Separation of Concerns

Figure 2 illustrates the container-level architecture of the proposed system, showing how consent governance responsibilities are distributed across modular components. The architecture separates identity management, consent logic, data storage, and audit functions to support scalability, interoperability, and privacy-by-design within heterogeneous healthcare environments.

Identity and credential services enable patient-controlled authentication using DIDs and VCs. Consent governance components manage consent states and enforce authorization rules. Blockchain-based logging services provide tamper-evident records of consent issuance, modification, and revocation, while personal health data remain stored exclusively in external institutional repositories under existing clinical and research governance controls. In this design, smart contracts maintain cryptographic references to consent state transitions and access authorization events, enabling verifiable auditability without storing personal health data on-chain.

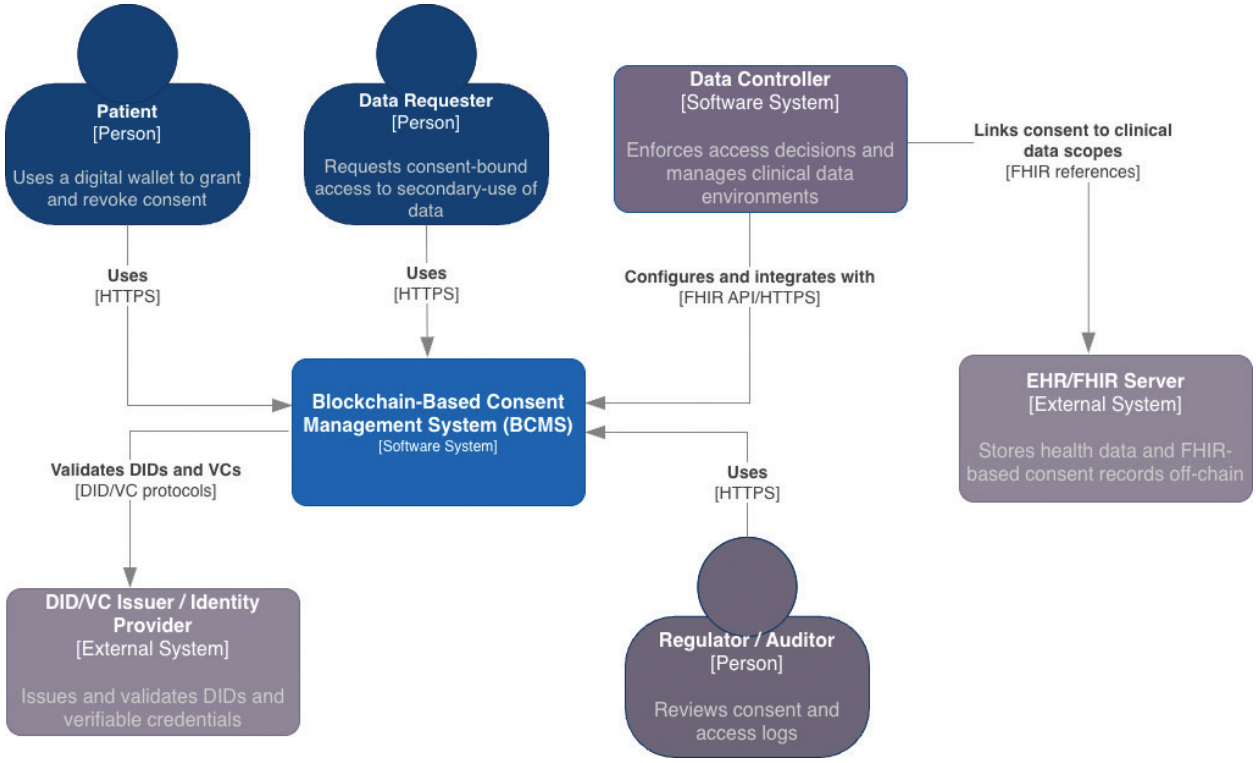

Fig. 1. C4 Level 1 system context diagram illustrating the primary actors involved in secondary health data use and their interactions. The diagram delineates trust and governance boundaries between patients, data requesters, consent governance services, institutional data repositories, and oversight authorities, highlighting where authorization decisions occur and where personal health data remain off-chain. DIDs: Decentralized Identifiers; VC: Verifiable Credentials; EHR: electronic health record; FHIR: Fast Healthcare Interoperability Resources.

Citation: Blockchain in Healthcare Today 2026, **9**: 491 - https://doi.org/10.30953/bhty.v9.491

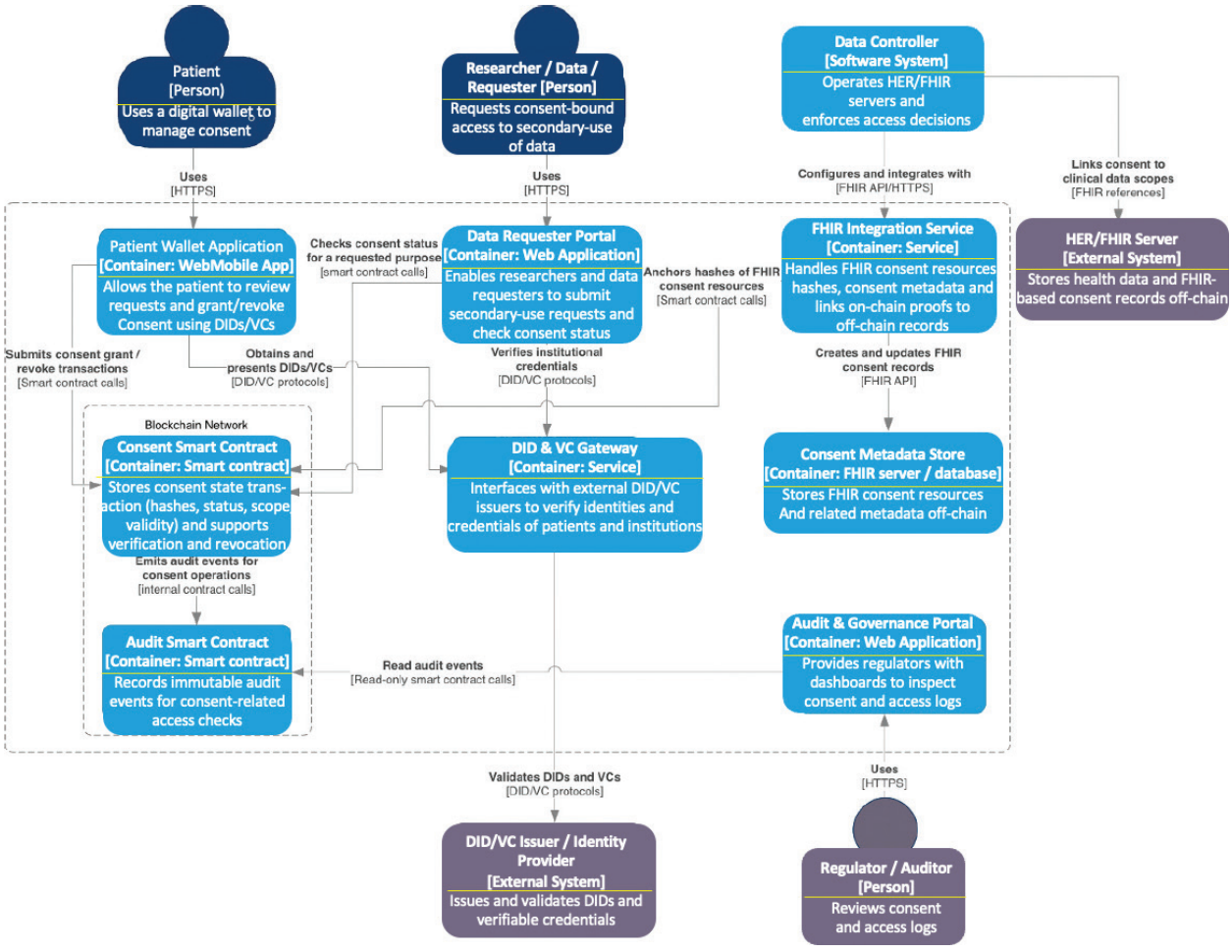

Fig. 2. C4 Level 2 container diagram showing the internal structure of the proposed architecture. On-chain components provide tamper-evident logging and consent state anchoring, while off-chain components handle identity management, consent metadata storage, and health data repositories. Authorization checks are enforced at institutional gateways based on the current consent state. DIDs: Decentralized Identifiers; VC: Verifiable Credentials; EHR: electronic health record; FHIR: Fast Healthcare Interoperability Resources.

This separation of concerns allows the architecture to function as a trust and governance layer over existing health information systems rather than as a replacement for clinical or research data infrastructures and enables incremental integration with minimal disruption to legacy systems.

Secondary-Use Access Request Workflow

To clarify the operational interaction between architectural components, Figure 3 illustrates the sequence of events during a secondary-use access request.

In this workflow, a data requester (for example a research institution or analytics service) submits a structured request to access patient data through an institutional access gateway. The gateway first performs decentralized identity verification using VCs presented by the requester.

The DID/VC gateway validates the credential using three steps. First, the cryptographic signature of the credential is verified against the issuer's public key referenced through the issuer's DID document. Second, the gateway checks whether the credential issuer is trusted within the applicable governance framework, such as an accredited healthcare organization or a recognized health data access authority. Third, the credential status is verified using standard revocation mechanisms, such as status lists or revocation registries.

Once the identity of the requester is verified, the gateway forwards the request to the consent governance service. The consent service queries the FHIR-based consent repository to determine whether valid consent exists for the requested data use.

The identity of the patient referenced in the request is mapped to the corresponding FHIR Consent resource using the patient identifier associated with the decentralized identity wallet. Consent enforcement logic then evaluates the relevant attributes, including purpose of use, authorized actors, permitted data categories, and validity period.

If the consent state is valid, the gateway authorizes access to the institutional health data repository. The access event and consent verification outcome are simultaneously recorded in the blockchain-based audit log as a tamper-evident governance record.

This workflow ensures that identity verification, consent enforcement, and audit logging occur in a coordinated and verifiable manner without exposing sensitive health data on-chain.

Dynamic Consent Lifecycle

A key design outcome is the representation of consent as a dynamic lifecycle rather than a one-time authorization event.

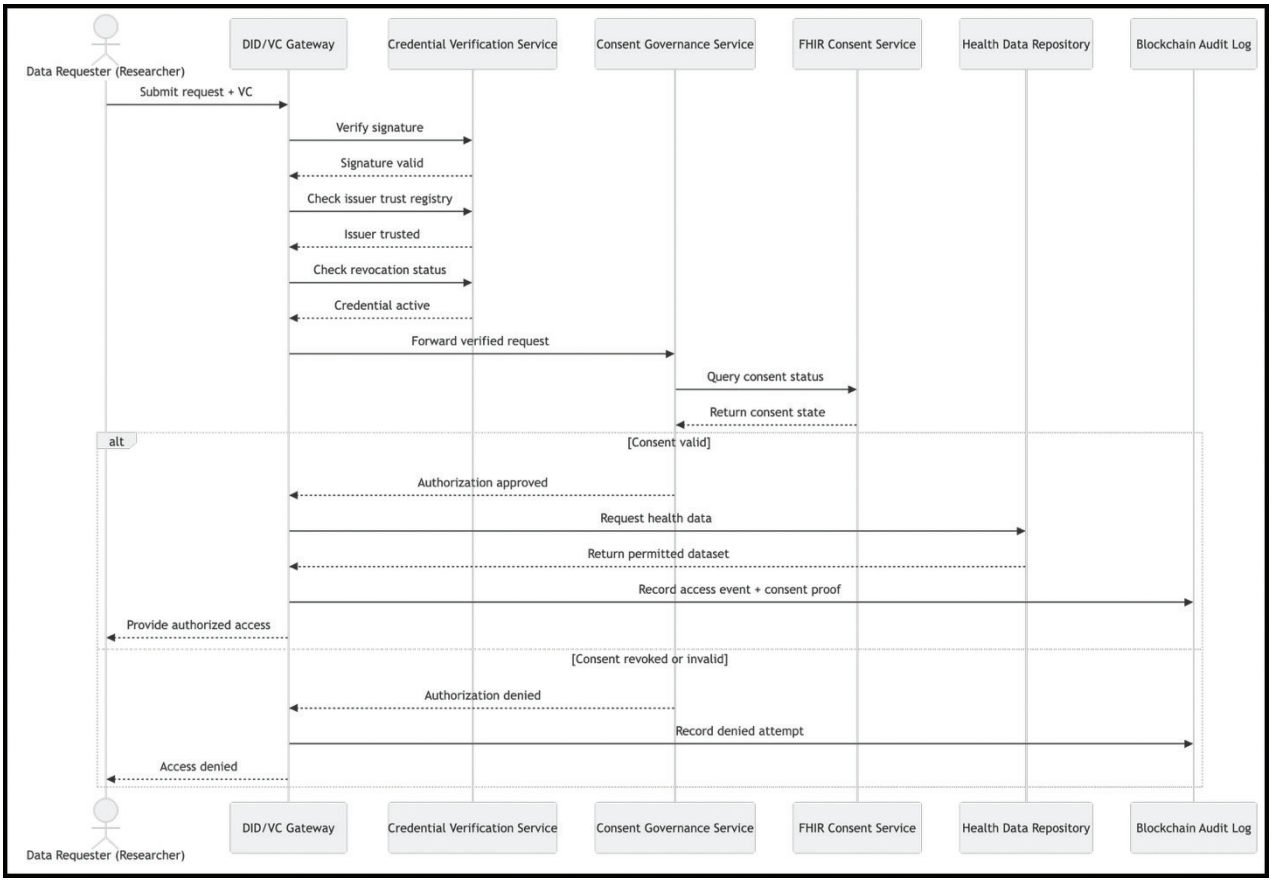

Fig. 3. Secondary-use consent authorization workflow. This sequence diagram illustrates the interaction between decentralized identity verification, consent governance services, HL7 FHIR consent repositories, institutional health data repositories, and blockchain-based audit logging during a secondary-use access request. The DID/VC gateway validates VCs through signature verification, issuer trust checks, and revocation status validation before querying the FHIR Consent service to determine whether access is authorized. DIDs: Decentralized Identifiers; VC: Verifiable Credentials; HL7 FHIR: Health Level Seven—Fast Healthcare Interoperability Resources.

The lifecycle consists of four coordinated stages: consent request, patient decision, consent enforcement, and consent revocation, which together operationalize continuous patient control.

Secondary-use requests are delivered to patients in a structured and transparent manner through their digital wallet. Patients can approve or deny requests based on clearly defined parameters, including purpose, scope, and duration. Approved consent decisions are recorded as standardized metadata and anchored using cryptographic references to ensure integrity and verifiability across distributed systems.

Consent enforcement is achieved by validating data access requests against the current consent state, ensuring that access is permitted only when authorization remains valid. Patients retain the ability to revoke consent at any time, triggering immediate invalidation of subsequent access attempts. All lifecycle events are recorded in tamper-evident logs, enabling post hoc verification without exposing personal health data or sensitive consent attributes.

By modeling consent as a continuous, stateful process, the architecture supports real-time governance of secondary data access and aligns technical enforcement with ethical expectations of ongoing patient agency.

Illustrative Execution Scenario of the Consent Lifecycle

To illustrate the operational behavior of the proposed architecture, this section presents a simplified execution scenario demonstrating how a secondary-use data request is processed within the system.

Consider a research institution requesting access to patient data for a public health study. The researcher first submits a structured access request through the institutional gateway, specifying the intended purpose of use, data categories, and requested duration.

The gateway requires the requester to present a VC representing institutional authorization to conduct research activities. The DID/VC gateway verifies the credential by validating the cryptographic signature, confirming the issuer's trust status within the applicable governance registry, and checking the credential's revocation status through a status list mechanism.

Once the requester identity is verified, the request is forwarded to the consent governance service. The service queries the HL7 FHIR Consent repository to determine whether the patient has granted valid consent for the requested purpose, data scope, and time period.

If a matching consent record exists and remains active, the authorization decision is returned to the institutional gateway. The gateway then retrieves the requested data from the health data repository while ensuring that only the permitted data elements are disclosed.

Simultaneously, the consent verification result and data access event are recorded in the blockchain-based audit log as

Citation: Blockchain in Healthcare Today 2026, **9**: 491 - https://doi.org/10.30953/bhty.v9.491

a cryptographic reference to the consent state and the authorized access transaction.

If the patient subsequently withdraws consent through their digital wallet, the consent state stored in the FHIR repository is updated, and a new consent-state reference is anchored on the blockchain. Future access requests referencing the revoked consent identifier are therefore rejected at the authorization gateway.

This illustrative execution scenario demonstrates how decentralized identity verification, standards-based consent representation, institutional authorization gateways, and blockchain-based audit logging interact to support dynamic and auditable consent management for secondary health data use.

Enforcement Scope and Governance Boundaries

To avoid overstating the effects of consent revocation in secondary-use ecosystems, the proposed architecture explicitly distinguishes between controls that can be technically enforced within system boundaries and those that depend on organizational governance and contractual obligations beyond the technical layer.

Technically enforced controls include: (1) authorization checks at institutional data-access gateways, where each access request is validated against the current consent state; (2) prevention of future access following consent withdrawal; (3) tamper-evident auditability of consent state transitions and access decisions via immutable logs; and (4) validation of consent constraints (purpose, scope, duration) at decision time.

Governance-dependent controls include: (1) management of downstream data copies after authorized export; (2) handling of derived artifacts such as analytic datasets or trained models; (3) obligations related to prior disclosures and publications; and (4) enforcement of data retention and deletion policies. These aspects require complementary governance instruments such as data-use agreements, institutional review processes, and enforcement by Health Data Access Bodies.

In particular, once health data have been incorporated into derived analytical artifacts, such as aggregated research datasets or machine learning models, complete technical revocation may no longer be feasible. For example, trained artificial intelligence models cannot easily be "un-trained" to remove the influence of previously authorized data. Similarly, de-identified datasets that have been disseminated to external researchers may remain in downstream analytical workflows even after consent withdrawal.

To address these limitations, the architecture supports complementary governance and provenance mechanisms. Provenance metadata frameworks, such as the World Wide Web Consortium Provenance (W3C PROV) model, can record lineage relationships between source datasets, derived datasets, and analytical outputs. This lineage information allows institutions and oversight authorities to identify which downstream artifacts were generated from specific source data.

In addition, regulatory governance mechanisms such as Health Data Access Bodies and formal data-use agreements can impose obligations on data recipients to document dataset lineage, restrict redistribution, and respect revocation-related governance policies. These instruments ensure that downstream data users remain accountable for respecting evolving consent conditions.

Even in cases where derived datasets or models cannot be technically modified after consent withdrawal, the blockchain-based audit log preserves verifiable records of consent states and access decisions. This immutable record enables post-revocation audits, supports forensic investigation of data-use histories, and facilitates the assignment of responsibility for potential misuse or policy violations.

In this article, real-time withdrawal therefore denotes real-time prevention of subsequent access and real-time auditability, rather than retroactive retrieval of data already disclosed under valid authorization.

Standards Integration and Interoperability Outcomes

The architecture integrates internationally recognized standards to ensure interoperability across heterogeneous health data ecosystems. Consent metadata are represented using HL7 FHIR, enabling alignment with EHR systems and research platforms and facilitating standardized exchange of consent states across organizational boundaries. Decentralized identity standards support patient-controlled authentication and verifiable authorization, while established audit principles guide traceable access logging in line with health information governance best practices.

By aligning consent representation and identity management with existing standards, the architecture supports cross-institutional and cross-border data reuse without requiring fundamental changes to underlying clinical systems. This interoperability outcome is particularly relevant in the context of the EHDS, where federated data exchange and secondary use are central objectives and where harmonized consent governance is a core enabler.

Table 5 summarizes the core standards and regulatory frameworks that underpin the proposed architecture at a conceptual level, while detailed representation and storage decisions for consent metadata are specified in Section 3.5.1.

These integration outcomes demonstrate that decentralized consent governance can be achieved without sacrificing compatibility with established health IT infrastructures, thereby lowering barriers to adoption in real-world healthcare environments.

FHIR Consent Representation and Storage Allocation

Consent decisions are represented using the HL7 FHIR Consent resource to enable interoperable exchange across institutional repositories and secondary-use services. To preserve data minimization, the full consent record is stored in an off-chain FHIR-native service, while integrity proofs and state references are anchored on-chain. These consent records can be implemented using national or institutional FHIR profiles derived from the HL7 FHIR Consent resource specification, enabling interoperability across heterogeneous health data infrastructures while allowing localized policy extensions.

Only a minimal interoperable subset of consent elements is required for governance enforcement and auditability. National or institutional FHIR profile extensions can therefore remain off-chain without affecting the integrity anchoring model or cross-system verifiability.

Table 5. Standards integration and interoperability outcomes.

Standard/Framework	Role in the architecture
HL7 FHIR	Standardized representation of consent metadata and linkage to electronic health record and research data systems
DIDs and Verifiable Credentials	Patient-controlled identity management and cryptographically verifiable consent authorization
ISO 27789	Principles for traceable, auditable access to electronic health records
GDPR and EHDS	Legal framework governing consent, accountability, and secondary use of health data

DIDs: Decentralized Identifiers; EHDS: European Health Data Space; FHIR: Fast Healthcare Interoperability Resources; GDPR: General Data Protection Regulation; HL7 FHIR: Health Level Seven—Fast Healthcare Interoperability Resources.

Table 6. Consent attributes to FHIR mapping.

Consent attribute	FHIR element	Storage location
Purpose of use	provision.purpose	Off-chain; hash anchored on-chain
Scope/category	scope, category	Off-chain
Patient	patient	Off-chain reference
Validity period	provision.period	Off-chain
Actors	provision.actor	Off-chain
Data scope	provision.data	Off-chain
Status	status	Off-chain with on-chain state anchoring

FHIR: Fast Healthcare Interoperability Resources.

Table 7. Regulatory alignment of architectural functions.

Architectural function	Regulatory requirement	Governance outcome
Consent revocation	GDPR Article 7(3); EHDS Article 33	Prevention of subsequent access requests and verifiable auditability of consent state changes within the system boundary
Audit logging	GDPR Article 30; EHDS Article 32	Tamper-evident, traceable records supporting accountability and regulatory oversight
Identity management	GDPR Article 4(11); EHDS Article 34	Explicit, patient-managed consent and privacy-preserving authentication
Data minimization	GDPR Article 5(1)(c)	No personal health data stored on-chain; cryptographic references only

GDPR: General Data Protection Regulation, EHDS: European Health Data Space.

This allocation ensures interoperability with FHIR-compliant systems while maintaining privacy-by-design and scalability. By anchoring only cryptographic references and consent state indicators on-chain, the architecture avoids storing personal or domain-specific consent metadata in the ledger, thereby aligning with GDPR data minimization principles and EHDS governance expectations.

Compliance and Governance Implications

The proposed architecture embeds regulatory compliance directly into its design through explicit alignment with the GDPR and the EHDS. Consent revocability, purpose limitation, and accountability are operationalized through architectural mechanisms rather than organizational policy alone or manual governance procedures.

Immutable consent logs support traceable access and regulatory oversight, while off-chain storage of health data ensures compliance with data minimization principles. Authorized oversight bodies can verify historical consent states and access decisions without accessing personal health data, supporting transparency, accountability, and public trust in secondary data-sharing practices across institutional and national boundaries.

By enabling demonstrable, technically enforced accountability, the architecture provides a concrete governance mechanism for EHDS-aligned secondary-use infrastructures and supports supervisory authorities in auditing data access practices.

Summary of Results

The results demonstrate that a modular, blockchain-enabled consent architecture can conceptually support dynamic consent lifecycle management, interoperability with existing health data infrastructures, and compliance with European regulatory requirements for the secondary use of health data. By positioning blockchain as a governance and audit mechanism rather than a data storage solution, and by integrating decentralized identity and health data standards, the architecture strengthens patient autonomy and trust while enabling responsible data reuse across distributed healthcare ecosystems. These design outcomes establish a foundation for future prototype implementation, usability evaluation, and real-world pilot studies within European digital health ecosystems and EHDS-aligned secondary-use infrastructures.

Taken together, the findings indicate that governance-oriented system design, grounded in standards and compliance-by-design principles, can bridge the gap between regulatory expectations and the technical realities of large-scale secondary health data sharing.

Discussion

Principal Findings

This study proposes a patient-centered, standards-based architecture for managing consent in the secondary use of health data, designed to support dynamic consent, auditability, and regulatory compliance within European digital health ecosystems. These findings directly reflect the defined design objectives. In particular, O1 is achieved through the dynamic consent lifecycle model, O2 through blockchain-based audit logging, O3 through HL7 FHIR and decentralized identity integration, and O4 through off-chain data storage and compliance-oriented architectural design. The primary contribution is not a software implementation but a governance-oriented architectural model that operationalizes patient consent as a continuous lifecycle rather than a static authorization event suitable for federated secondary-use environments.

Citation: Blockchain in Healthcare Today 2026, **9**: 491 - https://doi.org/10.30953/bhty.v9.491

By integrating blockchain-based audit logging with decentralized identity technologies and HL7 FHIR, the proposed architecture demonstrates how consent decisions can remain patient-driven while being enforceable and verifiable across distributed organizational boundaries. The results indicate that blockchain can function effectively as a trust and accountability layer, rather than as a data storage mechanism, thereby aligning technical design choices with legal and ethical requirements under the GDPR and the EHDS without introducing new central points of control.

Importantly, the findings suggest that combining standards-based interoperability with decentralized governance mechanisms can address long-standing tensions between scalability, patient autonomy, and regulatory accountability in secondary health data sharing.

Although the design emphasizes consent-driven governance to strengthen patient autonomy and transparency, the same architectural layer can document, enforce, and audit authorization decisions based on alternative lawful bases for secondary use, including opt-out regimes and legally mandated processing. By abstracting authorization logic from the underlying legal basis, the architecture supports consistent auditability and accountability across consent-based and non-consent-based secondary-use scenarios, in line with EU regulatory practice.

Comparison with Prior Work

Prior research on consent management in healthcare has explored a range of approaches, including broad consent, meta-consent, and dynamic consent platforms. While these models have advanced patient engagement and flexibility, most existing implementations rely on centralized infrastructures and institutional trust. As a result, they often lack verifiable auditability, real-time enforcement of consent withdrawal, and transparency across organizational or national boundaries.[13,14] For example, dynamic consent implementations enable ongoing patient interaction but still depend on backend enforcement and organizational control rather than decentralized, technically enforceable governance.

Blockchain-based approaches have been proposed to address some of these limitations, particularly in relation to audit logging, access transparency, and governance enforcement.[9,18] Early systems like MedRec illustrated the feasibility of using distributed ledgers to record access events and permission pointers in healthcare contexts, though they focused primarily on access logging rather than full consent lifecycle management under regulatory constraints.[17] Subsequently, frameworks have been introduced that leverage smart contracts to automate consent enforcement and traceability, emphasizing tamper-evident logs and regulatory compliance in healthcare environments.[16] However, many such frameworks remain conceptual or limited in scope, and only a small number explicitly integrate interoperability standards such as HL7 FHIR into blockchain-based consent and access workflows.[13]

Dynamic consent in blockchain contexts has also been explored in conceptual systematic reviews and protocols, which recognize blockchain's potential for patient empowerment and ongoing consent control but note a lack of empirical evidence on deployed systems.[15] These reviews underscore that most published work still resides at early research stages, with few best practices for robust, standards-aligned implementations.

More recent research has begun to articulate frameworks combining blockchain, smart contracts, and standards such as FHIR for consent and data exchange, though many are theoretical or pre-implementation reports, and some propose architectures that integrate privacy techniques such as zero-knowledge proofs to enhance privacy in data sharing agreements.[23] Additionally, research in[20] highlights how blockchain, self-sovereign identity, and DIDs can advance secure and self-determined health data sharing and consent tracking but also points out structural challenges to real-world adoption and governance.

In contrast, the architecture presented in this study explicitly targets the secondary use of health data and positions consent as a dynamic, patient-managed lifecycle rather than a static permission. Unlike centralized dynamic consent platforms,[16,17] the proposed model avoids reliance on institutional trust alone by introducing tamper-evident blockchain-based audit logging and technically enforced consent-state validation. Compared with early blockchain solutions like MedRec,[24] our approach embeds compliance with GDPR and EHDS requirements directly into design decisions such as consent revocability and purpose limitation. Relative to frameworks focusing on smart contracts for generic consent enforcement,[16] this work places stronger emphasis on interoperability by integrating HL7 FHIR for consent metadata representation and on privacy-by-design through off-chain storage and minimal on-chain metadata. Further, by incorporating decentralized identity wallets (DIDs/VCs), the architecture advances beyond prior blockchain-FHIR integration efforts toward a patient-controlled, standards-aligned consent governance model suitable for EHDS-aligned secondary-use infrastructures.[20]

Overall, existing approaches tend to optimize individual dimensions of consent management such as patient interaction, auditability, or automation without offering a unified solution that simultaneously supports dynamic lifecycle management, interoperability, regulatory compliance, and decentralized governance.

In addition to this comparison, the novelty of the proposed architecture lies in the integration of multiple governance and interoperability layers within a single consent management framework. Unlike earlier blockchain-based systems that primarily focus on access logging or static permission management, the proposed model explicitly supports a dynamic consent lifecycle aligned with European regulatory requirements for secondary health data use. The architecture combines decentralized identity mechanisms (DIDs and VCs) with standardized HL7 FHIR consent resources, enabling interoperable authorization decisions across institutional and national boundaries. Furthermore, by separating on-chain audit anchoring from off-chain storage of consent metadata and health data, the design aligns with GDPR data minimization principles while preserving tamper-evident governance. Finally, the architecture explicitly maps technical functions to EHDS governance requirements, positioning the model as a compliance-oriented infrastructure blueprint for secondary-use health data ecosystems rather than solely as a blockchain-based access control mechanism.

Implications for Digital Health Practice and Policy

The proposed architecture has several implications for digital health practice, governance, and policy. For patients, the model supports greater autonomy and transparency by enabling ongoing control over how health data are reused, including the ability to revoke consent at any time. This may help strengthen trust and willingness to participate in research and data-sharing initiatives, particularly in contexts involving cross-border or secondary data use where concerns about loss of control are most pronounced.

For researchers, public health authorities, and data-driven innovation initiatives, the architecture provides a clear and verifiable mechanism for requesting, validating, and enforcing consent, thereby reducing ambiguity and compliance risk. The integration of standardized consent metadata and decentralized identity also facilitates interoperability across heterogeneous health data environments and supports automated, policy-driven access governance.

From a policy and regulatory perspective, the architecture offers a concrete example of how compliance-by-design can be operationalized in digital health systems. By mapping architectural functions directly to regulatory requirements, the model demonstrates how emerging European health data governance frameworks can be supported through technical design rather than post hoc organizational controls or manual audit processes.

More broadly, the proposed model can inform the design of EHDS-aligned secondary-use services, data access bodies, and trust frameworks for digital wallets and VCs, contributing to the translation of regulatory principles into deployable infrastructures. In practice, the architecture is particularly relevant for research data platforms, hospital-led secondary-use services, and future EHDS-aligned data access infrastructures that require auditable authorization and patient-facing consent control.

To illustrate how the proposed architecture could operate in practice, consider a secondary-use research scenario involving multiple European stakeholders. A university research group submits a request to analyze anonymized clinical data related to cardiovascular disease across several hospitals. The request is first reviewed by a Health Data Access Body responsible for evaluating the legal basis, research purpose, and compliance with national and European governance requirements. Once the request is approved, institutional gateways at participating hospitals validate the authorization and verify the researchers' credentials using decentralized identity mechanisms.

Patients whose data may be included in the study receive consent requests through their digital health wallets or alternative consent interfaces supported by national eID systems or institutional patient portals. The consent governance service evaluates whether valid consent exists for the requested purpose and data scope using HL7 FHIR consent records. If authorization is confirmed, the institutional repositories release only the permitted datasets while recording the access decision in the blockchain-based audit log. Oversight authorities can subsequently verify that the research data access complied with both consent conditions and governance policies without accessing sensitive patient information.

This scenario demonstrates how decentralized identity verification, standards-based consent representation, and blockchain-based audit logging can operate within existing European governance frameworks to support transparent and accountable secondary-use health data access across institutional and national boundaries.

Limitations

This study has several limitations that should be considered when interpreting its findings. First, the proposed architecture is conceptual and has not been implemented or evaluated in a real-world deployment. As such, performance characteristics such as transaction latency, system throughput, and integration overhead were not empirically measured and remain theoretically reasoned based on design assumptions.

Second, the architecture assumes the availability of digital identity wallets and a baseline level of digital literacy among patients. In practice, disparities in access to technology and digital skills may limit adoption or require complementary support mechanisms to ensure equitable participation across diverse populations.

Third, while the architecture is aligned with HL7 FHIR and European regulatory frameworks, variability in national implementations of FHIR profiles and differences in institutional governance models may introduce integration challenges and require localized adaptation. Finally, governance aspects such as credential issuer trust frameworks, dispute resolution, and cross-border authority recognition are acknowledged but not explored in depth within the scope of this study.

Fourth, the proposal assumes the existence of a viable trust framework for decentralized identity in healthcare, including authorized issuers of VCs, revocation infrastructure, and interoperable verification policies across jurisdictions.[10]

Fifth, integration with existing data-access committees, Health Data Access Bodies, and institutional repositories may introduce non-trivial process and change-management overhead. Even with standards alignment, organizations may require policy updates, operational controls, and staff training to operationalize real-time consent withdrawal and audit verification within established governance workflows.

Finally, while patient wallets can strengthen autonomy, they may also increase cognitive load and risk of consent fatigue. User experience design, default policy templates, and assisted decision-making mechanisms will be necessary to ensure the system remains usable and equitable across differing levels of digital literacy and health literacy.

Trust Framework Assumption

The architecture assumes that VC issuers are authorized entities, such as national electronic identity (eID) providers, accredited healthcare organizations, or EHDS–aligned trust registries. It further assumes that credential verifiers apply explicit verification policies and that credential lifecycle management includes mechanisms for status and revocation checking. Governance anchors may therefore take the form of national or supranational registries defining issuer accreditation criteria, trust anchors, and verification rules.

To ensure cross-jurisdictional applicability, these trust dependencies are treated as pluggable components rather than

Citation: Blockchain in Healthcare Today 2026, 9: 491 - https://doi.org/10.30953/bhty.v9.491

hard-coded assumptions. This allows the architecture to be deployed under existing national health identity frameworks, accredited consortium-based governance models, or future EHDS-aligned trust infrastructures without requiring changes to the core consent and audit mechanisms.

Consent Fatigue and User Experience Considerations

While dynamic consent enhances patient autonomy, frequent or complex consent requests may lead to consent fatigue and reduced engagement over time. To mitigate this risk, the proposed architecture can support several user experience and governance mechanisms that simplify decision-making while preserving patient control.

First, the system supports consent policy templates that allow patients to predefine preferences for common secondary-use scenarios, such as public health research or academic studies. These templates may be stored within the patient's digital wallet or in a trusted consent template registry managed by the consent governance service. Templates define reusable consent parameters, including purpose of use, authorized actors, permitted data categories, and validity duration. Importantly, templates do not bypass consent verification mechanisms; instead, they populate HL7 FHIR Consent resource fields while preserving granular consent attributes required for regulatory compliance.

To ensure that templates do not weaken patient autonomy, several safeguards are implemented. Templates may include mandatory review prompts, requiring patients to confirm or adjust template parameters before authorization. In addition, template expiration rules ensure that predefined consent preferences must be periodically revalidated by the patient. These mechanisms maintain patient awareness of ongoing data-use permissions while reducing repetitive decision burdens.

Accessibility and digital inclusion are also important considerations for real-world deployment. The architecture therefore supports assisted-consent modes that allow patients to delegate consent management to trusted representatives when legally permitted. Such proxy delegation mechanisms may be implemented using VCs representing authorized caregivers or legal guardians. Additionally, institutional patient support portals may provide assisted consent workflows through healthcare providers or trusted intermediaries.

Finally, integration with national eID systems can provide lower-barrier authentication mechanisms for individuals who may not use specialized digital identity wallets. These complementary pathways help ensure that consent governance remains inclusive and accessible across diverse patient populations and digital literacy levels.

Security Governance and Forensic Auditability

While cryptographic identity verification and consent-state validation reduce many authorization risks, institutional access gateways remain potential targets for insider misuse or operational misconfiguration. To mitigate these risks, the architecture incorporates several complementary governance mechanisms.

First, secondary audit trails can be maintained at institutional gateways to record detailed access logs, including requester identity, requested datasets, authorization outcomes, and timestamps. These operational logs complement blockchain-based governance logs and enable fine-grained monitoring of system activity.

Second, anomaly-detection mechanisms can analyze access patterns to identify unusual behavior, such as excessive query volumes, repeated access to restricted datasets, or deviations from typical research workflows. Such monitoring can be implemented through automated analytics systems integrated with institutional security operations.

Third, federated governance models allow multiple participating institutions or regulatory authorities to independently verify blockchain-based audit logs. Because the ledger records cryptographic references to consent states and access events, oversight bodies can validate the integrity of authorization decisions without relying on a single institutional operator.

Finally, the immutable nature of blockchain logs supports forensic investigations following security incidents. Even if an institutional gateway were compromised or manipulated, the append-only ledger maintains verifiable records of consent issuance, revocation, and access decisions. Investigators can therefore reconstruct historical authorization events, identify unauthorized access attempts, and assign accountability for policy violations.

Future Research Directions

Future work should focus on translating the proposed architecture into a functional prototype to evaluate technical performance, usability, and interoperability in real-world settings. User-centered evaluations involving patients, researchers, and data governance bodies will be essential to assess usability, trust, and acceptance across diverse secondary-use scenarios.

Further research may also explore the integration of advanced privacy-preserving techniques, such as zero-knowledge proofs, to minimize metadata exposure during authorization checks and to enable verifiable compliance without revealing sensitive consent attributes. Extending the model to support governance of artificial intelligence applications such as tracking consent-bound datasets and auditing AI training pipelines represents another promising direction.

Finally, cross-border pilot studies aligned with the rollout of the EHDS would provide valuable insights into scalability, policy alignment, and institutional adoption across diverse healthcare systems and help validate the feasibility of federated consent governance under real regulatory conditions.

Conclusions

This study presents a conceptual, patient-centered architecture for managing consent in the secondary use of health data. By integrating decentralized identity, standards-based consent metadata, blockchain-enabled audit logging, and off-chain data storage, the proposed model supports dynamic consent, interoperability, and regulatory compliance without compromising patient privacy or data minimization principles.

Although the architecture remains conceptual, it provides a practical and policy-relevant blueprint for future implementations aimed at enabling trustworthy secondary health data use in European digital health ecosystems. The findings highlight the potential of combining governance-oriented system design

with emerging digital health standards to strengthen patient autonomy, transparency, and accountability in data-driven healthcare innovation under GDPR and EHDS frameworks.

In practice, the primary beneficiaries of this blueprint are: (1) health data platforms and data spaces implementing secondary-use governance services, (2) hospitals and research infrastructures seeking auditable consent handling, and (3) policy and standards stakeholders defining trust frameworks for wallets, DIDs/VCs, and EHDS-aligned access auditing. A near-term implementation path would be a pilot integrating a FHIR-based consent service with an institutional repository and a limited-scope blockchain audit layer, followed by usability testing of wallet consent flows and validation with data-access governance bodies to demonstrate feasibility and inform large-scale adoption.

Overall, this work contributes a standards-aligned, compliance-by-design architectural foundation for patient-driven consent governance and offers a concrete step toward operationalizing trustworthy secondary health data sharing in Europe.

Funding

This work is supported by the Blockchain.PT (PRR—RE-C05-i01.02: AGENDAS/ALIANÇAS VERDES PARA A INOVAÇÃO EMPRESARIAL) and EDU-CARE projects. It was also supported by national funds through FCT - Fundação para a Ciência e a Tecnologia, I.P., under projects/supports UID/6486/2025 (https://doi.org/10.54499/UID/06486/2025) and UID/PRR/6486/2025 (https://doi.org/10.54499/UID/PRR/06486/2025).

Financial and Non-Financial Relationships and Activities

None.

Contributions

Sudip Phuyal: Conceptualization, writing original draft, revision, methodology. Manila Bhandari: Writing original draft, revision. Rabindra Bista: Revision, supervision, project management. João Carlos Ferreira: Revision, supervision, project management, funding acquisition.

Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories

Contact the corresponding author.

Application of AI-Generated Text or Related Technology

None used.

References

1. Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: a patient interface for twenty-first century research networks. Eur J Hum Genet. 2015;23:141–6. https://doi.org/10.1038/ejhg.2014.71
2. Charles WM, van der Waal MB, Flach J, Bisschop A, van der Waal RX, Es-Sbai H, et al. Blockchain-based dynamic consent and its applications for patient-centric research and health information sharing: protocol for an integrative review. JMIR Res Protoc. 2024;13:e50339. https://doi.org/10.2196/50339
3. Rodríguez-Mejías S, Degli-Esposti S, González-García S, Parra-Calderón CL. Toward the European Health Data Space: the IMPaCT-data secure infrastructure for EHR-based precision medicine research. J Biomed Inform. 2024;156:104670. https://doi.org/10.1016/j.jbi.2024.104670
4. Draft guideline to health data access bodies: how to implement opt-out from secondary use of electronic health data [Internet]. TEHDAS2 Joint Action; n.d. [cited 2025 Dec 25]. Available from: https://tehdas.eu/wp-content/uploads/2025/09/draft-guideline-to-health-data-access-bodies-how-to-implement-opt-out-from-secondary-use-of-electronic-health-data.pdf
5. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance) [Internet]. 2025 [cited 2025 Aug 14]. Available from: http://data.europa.eu/eli/reg/2025/327/oj/eng
6. Consumers, Health, Agriculture and Food Executive Agency. Assessment of the EU Member States' rules on health data in the light of GDPR [Internet]. Publications Office, LU; 2021 [cited 2025 Dec 9]. Available from: https://data.europa.eu/doi/10.2818/546193
7. Elangovan D, Long CS, Bakrin FS, Tan CS, Goh KW, Yeoh SF, et al. The use of blockchain technology in the health care sector: systematic review. JMIR Med Inform. 2022;10:e17278.
8. Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. Systems. 2023;11:38.
9. Choudhury O, Sarker H, Rudolph N, Foreman M, Fay N, Dhuliawala M, et al. Enforcing human subject regulations using blockchain and smart contracts. Blockchain Healthc Today. 2018;1:10. https://doi.org/10.30953/bhty.v1.10
10. Satybaldy A, Hasselgren A, Nowostawski M. Decentralized identity management for e-health applications: state-of-the-art and guidance for future work. Blockchain Healthc Today. 2022;5(S1):195. https://doi.org/10.30953/bhty.v5.195
11. Benchoufi M, Ravaud P. Blockchain technology for improving clinical research quality. Trials. 2017;18:335. https://doi.org/10.1186/s13063-017-2035-z
12. Agbo CC, Mahmoud QH, Eklund JM. Blockchain technology in healthcare: a systematic review. Healthcare. 2019;7:56.
13. Carter G, Chevellereau B, Shahriar H, Sneha S. OpenPharma blockchain on FHIR: an interoperable solution for read-only health records exchange through blockchain and biometrics. Blockchain Healthc Today. 2020;3:120. https://doi.org/10.30953/bhty.v3.120
14. Tabari P, Costagliola G, De Rosa M, Boeker M. State-of-the-art fast healthcare interoperability resources (FHIR)–based data model and structure implementations: systematic scoping review. JMIR Med Inform. 2024;12:e58445.
15. Shaikh M, Memon SA, Ebrahimi A, Wiil UK. A systematic literature review for blockchain-based healthcare implementations. Healthcare. 2025;13:1087.
16. Lee AR, Koo D, Kim IK, Lee E, Yoo S, Lee H-Y. Opportunities and challenges of a dynamic consent-based application: personalized options for personal health data sharing and utilization. BMC Med Ethics. 2024;25:92. https://doi.org/10.1186/s12910-024-01091-3
17. Xiong E, Bonner C, King A, Bourne ZM, Morgan M, Tolosa X, et al. Insights from the development of a dynamic consent platform for the Australians Together Health Initiative (ATHENA) Program: interview and survey study. JMIR Form Res. 2024;8:e57165. https://doi.org/10.2196/57165
18. Mak BC, Addeman BT, Chen J, Papp KA, Gooderham MJ, Guenther LC, et al. Leveraging blockchain technology for informed consent process and patient engagement in a clinical trial pilot. Blockchain Healthc Today. 2021;4:182. https://doi.org/10.30953/bhty.v4.182
19. Frempong D, Benson CE, Oyasiji O, Okesiji A. Blockchain-enabled consent management in healthcare: a framework for enforcing privacy preferences and regulatory compliance. Health (N.Y.). 2024;3:5.
20. Welzel C, Ostermann M, Smith HL, Minssen T, Kirsten T, Gilbert S. Enabling secure and self determined health data sharing and consent management. Npj Digit Med. 2025;8:560. https://doi.org/10.1038/s41746-025-01945-z
21. Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S. A design science research methodology for information systems research. J Manag Inf Syst. 2007;24:45–77. https://doi.org/10.2753/MIS0742-1222240302

22. Chhetri TR, Kurteva A, DeLong RJ, Hilscher R, Korte K, Fensel A. Data protection by design tool for automated GDPR compliance verification based on semantically modeled informed consent. Sensors. 2022;22:2763.
23. Li K, Lohachab A, Dumontier M, Urovi V. Privacy preservation in blockchain-based healthcare data sharing: a systematic review. Peer-Peer Netw Appl. 2025;18:302. https://doi.org/10.1007/s12083-025-02148-9
24. Ekblaw AC. MedRec: blockchain for medical data access, permission management and trend analysis [Internet]. PhD thesis, Massachusetts Institute of Technology, 2017 [cited 2025 Dec 24]. Available from: https://dspace.mit.edu/handle/1721.1/109658