Blockchain-Based Dynamic and Revocable Consent for Secondary Health Data Use: Systematic Review

Sudip Phuyal, M.Sc.[1], Manila Bhandari, M.Sc.[1], Rabindra Bista, PhD[2], João Carlos Ferreira, PhD[1,3,4,*]

[1]*Information Sciences, Technology and Architecture Research Center (ISTAR), University Institute of Lisbon (ISCTE-IUL), 1649-026 Lisbon, Portugal*
[2]*Department of Computer Science and Engineering, Kathmandu University, Dhulikhel 45200, Nepal*
[3]*Faculty of Logistics, Molde University College, 6410 Molde, Norway*
[4]*Inov Inesc Inovação - Instituto de Novas Tecnologias, 1000-029 Lisbon, Portugal*

Corresponding author:
João Carlos Ferreira
Faculty of Logistics, Molde University College
6410 Molde, Norway
Phone: +47 71 21 40 00
Email: joam@himolde.no

Abstract:

Background: The secondary use of health data holds substantial potential for advancing biomedical research, strengthening population health analytics, and enabling AI–driven decision support. Yet ensuring that such reuse respects patient autonomy, privacy, and regulatory obligations remain a major challenge. Conventional consent mechanisms are typically static, difficult to revoke, and offer limited transparency or accountability after data disclosure.

Objective: This review aimed to systematically examine blockchain-based frameworks that enable dynamic, auditable, and revocable consent for the secondary use of health data.

Methods: A structured literature search was conducted in PubMed, Scopus, and Web of Science covering the period 2020–2025. Following PRISMA guidelines, 55 peer-reviewed studies meeting predefined inclusion criteria were analyzed. Data extraction focused on four dimensions: (1) consent lifecycle management; (2) auditability and traceability; (3) usability and patient empowerment; and (4) legal and ethical alignment.

Results: Findings indicate that blockchain technologies provide a robust foundation for automating consent lifecycles, ensuring immutable auditability, and enabling decentralized patient control. Most frameworks employed smart contracts, DIDs (decentralized identifiers), and VCs (verifiable credentials) to implement programmable and verifiable consent processes. Nevertheless, key challenges persist, including limited usability testing, complexities in real-time revocation propagation, interoperability gaps with clinical systems, and tensions with regulatory requirements such as the GDPR (General Data Protection Regulation) right to erasure. Only a small subset of studies reported real-world deployments or user-centered evaluations.

Conclusions: Blockchain offers substantial promise for improving the trustworthiness, transparency, and accountability of consent management for secondary health data use. However, wider adoption requires human-centered design approaches, stronger interoperability through standards such as FHIR, verifiable credentials, and consent receipts, and clearer legal guidance for compliance. Future research should prioritize integrating blockchain-enabled consent infrastructures into national and cross-border digital health ecosystems such as the EHDS (European Health Data Space) to support secure, patient-controlled, and ethically governed secondary data use.

Keywords: Blockchain; Dynamic Consent; Revocable Consent; Healthcare Data Sharing; Data Privacy; Auditability; GDPR (General Data Protection Regulation); EHDS (European Health Data Space)

Introduction

The digitalization of healthcare has expanded how patient data are used and shared, raising important questions about consent, privacy, and individual control. While large-scale reuse of health data enables advances in biomedical research, population health analytics, and data-driven innovation, traditional consent models often fall short in this evolving landscape [1,2]. Conventional approaches are typically static, difficult to revoke, and provide limited transparency once data have been shared, making them poorly suited for continuous, cross-institutional, and cross-border secondary use of health data.

Recent regulatory developments, notably the European Health Data Space (EHDS) Regulation, further reinforce the need for interoperable and trustworthy consent infrastructures for secondary use of health data. Acting as lex specialis over the General Data Protection Regulation (GDPR) in this context, the EHDS introduces dedicated governance mechanisms [3], access frameworks, and infrastructure requirements for health data reuse within the European Union. While the GDPR establishes baseline principles

for lawful processing, including informed and revocable consent, the EHDS places additional emphasis on harmonized procedures, institutional accountability, and cross-border operability [4].

Recent implementation guidance further clarifies how patient rights under the EHDS should be operationalized in practice. In particular, the TEHDAS guideline for Health Data Access Bodies specifies common principles and procedures for implementing opt-out mechanisms for the secondary use of electronic health data, emphasizing transparency, harmonized national processes, and citizen-facing tools to exercise opt-out rights [3]. This guidance highlights that EHDS compliance depends not only on legal provisions but also on concrete organizational and technical processes capable of managing consent and opt-out at scale.

At the same time, emerging technologies such as blockchain and decentralized identity offer new architectural possibilities for enforcing consent policies, maintaining immutable audit trails, and enabling patient-centric control without reliance on central intermediaries [5–7]. Blockchain-based systems can provide tamper-evident records, shared governance across institutions, and programmable enforcement of consent conditions through smart contracts, while decentralized identity mechanisms allow individuals to retain control over their identifiers and consent credentials.

Several recent surveys have explored blockchain in healthcare or digital consent in isolation; however, they typically address broad application domains or focus on usability, ethical, or governance perspectives without systematically analyzing how blockchain-based architectures support dynamic and revocable consent specifically for the secondary use of health data. As a result, there remains a fragmented understanding of how consent lifecycles are technically implemented, how revocation is enforced across distributed systems, and how such frameworks align with evolving regulatory requirements under the GDPR and the EHDS [6–10]. This gap motivates the present systematic review.

Unlike prior reviews that examine blockchain in healthcare broadly or address digital consent primarily from ethical or governance perspectives, this review analyses dynamic and revocable consent as an enforceable lifecycle across distributed systems, integrating architectural, operational, usability, and regulatory dimensions.

Accordingly, the aim of this systematic review is to examine and synthesize blockchain-based frameworks that support dynamic, auditable, and revocable consent for the secondary use of health data. Specifically, this review analyses how existing approaches implement consent lifecycle management, enable auditability and traceability, support patient empowerment and usability, and align with legal and ethical requirements under the GDPR and the emerging European Health Data Space (EHDS). By consolidating evidence from peer-reviewed studies published between 2020 and 2025, this review seeks to identify prevailing architectural patterns, implementation gaps, and priority directions for future research and real-world deployment.

This paper is organized as follows. The Methods section describes the systematic review protocol, including the search strategy, eligibility criteria, and data extraction and synthesis procedures. The Results section presents the findings of the review, organized around key analytical dimensions related to consent lifecycle management, auditability, usability, and legal–ethical alignment. The Discussion interprets these findings in relation to existing literature, regulatory frameworks, and practical implications for the secondary use of health data.

Background and rationale

The rapid advancements in digital technology over the past three decades have led to the emergence of digital health, which is revolutionizing healthcare [11]. The digital transformation of healthcare has redefined how clinical and research data are collected, managed, and reused. With EHRs (Electronic Health Records) and other digital health systems being adopted so quickly, the data of healthcare has grown exponentially [12]. The EHRs, biobanks, and data-driven analytics platforms now form the backbone of modern healthcare systems by supporting clinical decision-making, personalized medicine, and population-level insights. Global policy initiatives, such as the World Health Organization's Global Strategy on Digital Health [2], emphasize the need for secure and interoperable infrastructures that enable the ethical data exchange and innovation.

Alongside this advancement, the secondary use of health data beyond direct patient treatment has become a key component of biomedical research, AI model development, and public-health surveillance [1]. However, these benefits raise the fundamental questions about patient autonomy, privacy, and consent governance. Legal frameworks like the GDPR require that personal data be handled transparently. They also specify that consent must always be specific, informed, and easy to withdraw [13]. In the European Union, the recently adopted European Health Data Space (EHDS) Regulation further establishes a dedicated legal framework for the secondary use of health data, acting as lex specialis over the GDPR in this domain and introducing cross-border governance and access mechanisms [4].

Despite these regulatory advances, current consent management models remain largely static [14]. Usually, the individuals sign a one-time authorization form that gives them data controllers general authorization to reuse their data, but they aren't given tools to control or withdraw their consent in a more precise way [15]. The centralized databases used for storing consent records often suffer from a lack of transparency and auditability. Also, they struggle to maintain real-time synchronization across the institutions, which creates single points of failure and reduces overall accountability. These weaknesses highlight the need for systems that will support continuous, verifiable, and user-driven consent throughout the data lifecycle.

From a technical perspective, these requirements challenge traditional centralized architectures and motivate the exploration of distributed trust infrastructures that can provide tamper-evident records, shared governance, and automated enforcement of consent policies across organizational boundaries.

In this context, blockchain and distributed ledger technologies (DLTs) have emerged as promising enablers due to their inherent properties of immutability, decentralization, and programmable logic. However, the choice of blockchain deployment model is critical in healthcare settings. Public, permissionless blockchains offer high transparency but raise concerns regarding scalability, governance, and the exposure of even pseudonymized metadata on global infrastructures, which may conflict with data minimization and purpose limitation principles.

Consequently, most healthcare-oriented frameworks favor permissioned or consortium DLTs, where participating nodes are operated by trusted healthcare authorities or institutions and where fine-grained access control and governance mechanisms can be enforced. Such models better align with regulatory expectations under GDPR and EHDS, while still enabling shared auditability and decentralized trust. These considerations underscore the need for consent management solutions that are not only legally compliant but also technically capable of operating in distributed, cross-institutional healthcare ecosystems. This background motivates the investigation of blockchain-based frameworks as potential trust layers for enabling dynamic, auditable, and revocable consent in the secondary use of health data.

In this context, blockchain-based architectures are increasingly explored as trust layers for dynamic, auditable, and revocable consent in cross-institutional healthcare ecosystems. However, their suitability strongly depends on the underlying deployment model and its regulatory implications.

Blockchain Deployment Models and Regulatory Constraints

Although blockchain technologies are frequently proposed as trust infrastructures for healthcare consent management, the choice of deployment model is critical. Public, permissionless blockchains, while offering high transparency and openness, are generally unsuitable for managing consent-related metadata in healthcare settings. Even when only pseudonymized identifiers, public keys, or decentralised identifiers (DIDs) are stored on-chain, the global replication of such metadata across open infrastructures lacks a clear need-to-know justification and may conflict with the GDPR principles of data minimization and purpose limitation.

Consequently, most healthcare-oriented consent management frameworks adopt permissioned or consortium-based distributed ledger technologies, where participating nodes are operated by trusted healthcare institutions, public authorities, or regulated intermediaries. These models enable fine-grained access control, governance, and institutional accountability, while still preserving shared auditability and tamper-evident records across organizational boundaries. Such architectural choices align more closely with GDPR requirements and with the governance expectations introduced by the European Health Data Space (EHDS) framework for the secondary use of health data.

Evolution of Consent and the Need for Dynamic Models

Traditional consent models were designed for one-time clinical visits or specific research studies [15,16]. In an era of continuous data flows and distributed analytics, these static approaches have become increasingly inadequate. Individuals rarely could modify or revoke consent as data are repurposed for new studies, shared across borders, or integrated into AI training pipelines [17]. This gap between what patients expect and what technology currently delivers can weaken trust in the digital-health ecosystems.

To address these concerns, dynamic consent was introduced as both an ethical and technical solution that allows individuals to modify, refine, or revoke their data-sharing choices at any time through the user-friendly interactive platforms [18]. By enabling ongoing engagement and communication between data subjects and controllers, dynamic consent promotes transparency, autonomy, and contextual decision-making. It also aligns with key principles of the GDPR, particularly Article 7, which ensures revocability, and Article 17, which gives individuals the right to have their data deleted. Within the European context, these principles are further operationalized for secondary use through the EHDS Regulation, which emphasizes patient rights, governance and cross-border data reuse under harmonized access mechanisms.

However, unlike primary use where consent is often the main legal basis, the EHDS introduces a governance model for secondary use in which data access may rely on specific legal bases but remains subject to a citizen's right to opt out. The TEHDAS guideline elaborates how Health Data Access Bodies should implement such opt-out mechanisms in practice, including registries and user interfaces for objections. This distinction is crucial for blockchain-based dynamic consent systems, which must interoperate with opt-out governance rather than assume that consent alone governs secondary use [3].

In contrast, most dynamic-consent implementations rely on centralized architectures that provide limited verifiability and poor interoperability across institutions. These systems may log user actions but cannot guarantee immutability, traceability, or real-time enforcement of revocation [19]. As secondary use increasingly involves multi-institutional and cross-border data flows, such limitations pose not only technical but also governance and compliance challenges. In particular, the lack of automated propagation of consent changes across distributed data custodians undermines the practical realization of revocability required by both GDPR and EHDS.

As secondary data use expands across jurisdictions and organizations, these limitations pose both technical and ethical challenges. This evolution highlights the need for consent infrastructures that can (i) maintain a shared and tamper-evident history of consent decisions, (ii) support fine-grained and time-bound authorizations, and (iii) enable verifiable enforcement of revocation across organizational boundaries.

These requirements motivate the exploration of blockchain-based approaches as potential enablers of dynamic, auditable, and decentralized consent management in healthcare.

Blockchain Foundations for Dynamic Consent

Blockchain offers architectural features that can address many of the limitations of centralized consent management [5]. Consent events such as granting, updating, and revoking permissions can be recorded in a tamper-proof manner verifiable by all the participants' nodes, which is immutability, transparency, and decentralization. These properties enable shared trust across organizations without relying on a single central authority.

Smart contracts are self-executing programs that are stored on the blockchain, that can automatically manage consent by granting or withdrawing access based on predefined conditions, such as specific timeframes or user decisions [20]. This makes it possible to handle consent in real time, reducing the need for third-party involvement and manual reconciliation between data controllers.
Other technologies, like DIDs and VCs, further enhance this process by enabling individuals to control their own digital identities [21]. With DIDs, users can create and manage their own digital identities without depending on the centralized systems. Meanwhile, VCs also make it possible to issue and share digitally signed proofs, such as consent records, which others can verify without revealing unnecessary personal information. Together, these tools enable a privacy-preserving, patient-centric consent framework where individuals maintain verifiable control over their data without exposing personal identifiers on-chain.
In most of the cases, blockchain is used as a coordination and auditing layer rather than a data-storage layer. The sensitive health information remains off-chain, while only hashed references, metadata and consent proofs are recorded on the ledger. This hybrid design supports GDPR's principles such as, data minimization and purpose limitation, and is also aligned with EHDS expectations for interoperable and trustworthy secondary-use infrastructures.
Accordingly, hybrid on-chain/off-chain architectures represent a baseline design pattern across healthcare blockchain systems, adopted from early proposals to recent implementations to address scalability and privacy constraints.
Although these technologies show potential for creating secure, adaptable, and revocable consent systems, it remains unclear how well they perform in real healthcare environments. Challenges persist in synchronizing on-chain consent states with off-chain policy enforcement points, ensuring timely revocation propagation, and integrating with existing health information systems. This highlights the need for a comprehensive review of current research to examine how the blockchain is being applied to dynamic consent and to consider the technical, ethical, and legal issues accompany it.

Identified Research Gaps

Blockchain and consent management have each been widely studied within digital health research. However, their intersection, particularly with respect to dynamic and revocable consent for the secondary use of health data remains insufficiently explored. Most blockchain-focused studies adopt a broad perspective, emphasizing applications such as electronic health record management, supply chain traceability, or digital identity, while treating consent as a static or peripheral feature. These approaches rarely conceptualize consent as a programmable lifecycle, enabling patients to grant, monitor, modify, and revoke permissions over time. In contrast, research on dynamic consent has predominantly emerged from ethical, legal, and user-experience perspectives, emphasizing patient autonomy, transparency, and trust. While this body of work provides important insights into participatory consent models, it often lacks a detailed examination of the technical infrastructures required to operationalize such models at scale. Key aspects including verifiable audit trails, enforceable revocation, interoperability across heterogeneous data custodians, and tamper-resistant governance mechanisms are seldom addressed in depth.
Across the primary literature, blockchain-based proposals for consent management are highly heterogeneous, spanning domains such as clinical trials, personal health records, genomics, and health information exchange. Despite this diversity, there is a notable lack of systematic synthesis focused specifically on secondary-use governance, where consent must be enforceable across institutional and jurisdictional boundaries and over extended time horizons. As a result, the design patterns, architectural trade-offs, and operational limitations of blockchain-enabled dynamic consent systems for secondary health data reuse remain poorly consolidated.
More recent studies have proposed frameworks combining blockchain with decentralized identity technologies, including decentralized identifiers (DIDs) and verifiable credentials (VCs). However, these approaches vary considerably in architectural design, regulatory assumptions, and levels of empirical validation. Few studies move beyond proof-of-concept implementations to evaluate performance in realistic cross-institutional or cross-border settings. In particular, automated revocation propagation, latency guarantees, coupling with off-chain policy enforcement points, and scalability under operational workloads remain weakly demonstrated.
Finally, although alignment with the General Data Protection Regulation (GDPR) is frequently asserted, the implications of the European Health Data Space (EHDS) Regulation as lex specialis for secondary use introducing dedicated governance bodies, access authorization mechanisms, and cross-border infrastructures are only sporadically addressed. This creates uncertainty regarding how blockchain-based consent models can integrate with emerging European data space architectures.
Accordingly, this study addresses these gaps by providing a PRISMA-based systematic review of literature published between 2020 and 2025, applying a structured analytical framework and quality assessment to evaluate blockchain-based dynamic consent architectures for secondary use of health data. By focusing on consent lifecycle management, auditability, usability evidence, and legal–ethical alignment, this review consolidates fragmented evidence and identifies the technical, evaluative, and governance limitations constraining the operational maturity of existing approaches.

Related work and critical comparison with existing reviews

Several recent reviews and surveys have examined blockchain and consent in healthcare from complementary but partial perspectives. However, none provide a unified analysis of dynamic and revocable consent lifecycles for secondary health data use, grounded simultaneously in blockchain-based enforcement mechanisms and emerging European regulatory requirements.
For instance, Hang et al. [6] review blockchain applications in clinical trials, emphasizing transparency and traceability, but treat consent primarily as a supporting mechanism rather than as a programmable lifecycle with explicit revocation semantics. Similarly, Baysal et al. [7] and other broad surveys map blockchain-based healthcare systems across diverse use cases, yet do not isolate

consent management for secondary use as a distinct analytical focus, nor do they assess enforceability or governance implications in depth.

From the consent-oriented literature, Schmidt et al. [8] present a scoping review of informed consent in digital health, identifying challenges related to consent acquisition and management. However, this work does not engage with blockchain architectures, smart contracts, or decentralized enforcement mechanisms. Likewise, Kassam et al. [9] and Cumyn et al. [10] synthesize patient and public perspectives on digital consent and transparency in secondary data use, offering valuable socio-ethical insights but without examining technical design choices or system-level trade-offs.

Other recent surveys, including Phuyal et al. [1], provide comprehensive overviews of blockchain in healthcare but do not analyze consent lifecycles, revocation propagation, or patient-controlled secondary-use governance. Across these reviews, regulatory considerations are typically limited to high-level discussions of GDPR compliance, with minimal treatment of the EHDS Regulation and its implications for secondary-use authorization, governance bodies, and cross-border interoperability.

To situate the present review within this landscape, Table 1 provides a structured comparison of recent review and survey papers intersecting blockchain, digital consent, and secondary use of health data. As summarized, existing reviews either focus broadly on blockchain applications without analyzing consent lifecycle enforceability or examine digital consent without addressing blockchain-based technical enforcement and secondary-use governance. In contrast, this review uniquely integrates (i) smart-contract–based consent lifecycle management, (ii) auditability and traceability mechanisms, (iii) usability and empirical evaluation evidence, and (iv) legal alignment with both GDPR and the EHDS Regulation, supported by a PRISMA methodology and formal quality assessment across 55 studies.

This comparative analysis demonstrates that the present review does not duplicate prior surveys, but instead provides an integrative assessment of consent lifecycle enforceability and governance readiness for secondary health data use, which has not been systematically examined in earlier secondary studies.

Taken together, prior reviews reflect the gradual evolution of consent research from static, paper-based authorization toward digital and dynamic consent models, and more recently toward decentralized and blockchain-enabled infrastructures. Early work on dynamic consent primarily emphasized ethical engagement, communication, and patient trust, while blockchain-focused healthcare surveys concentrated on data integrity, traceability, and access control. However, these strands have largely developed in parallel. As a result, the technical enforceability of dynamic and revocable consent across distributed systems, particularly for secondary use of health data, has remained insufficiently synthesized in the literature.

Table 1. Comparison of This Review with Recent Related Surveys

Review	Scope	Blockchain focus	Dynamic /Revocable Consent	Secondary Use Focus	EHDS/GDPR Analysis	Usability & Empirical Eval	Quality Assessment	This Review's Added Value
Hang et al. (2022) [6]	Blockchain in clinical trials	Yes	Yes	Focused on Trials	GDPR Only	No	No	Lacks lifecycle & revocation analysis
Baysal et al. (2023) [7]	Multivocal blockchain in healthcare	Yes	Yes	Broad	No	No	Yes	Broad mapping, no consent depth
Schmidt et al. (2025) [8]	Digital health consent (scoping)	Partial	Yes	Yes	GDPR only	No	No	No blockchain architecture analysis
Kassam et al. (2023) [9]	Patient perspectives on digital consent	No	Yes	Yes	No	Yes	No	Human factors only
Cumyn et al. (2023) [10]	Transparency in secondary use	No	Partially	Yes	Yes	Yes	No	Governance without tech
Phuyal et al. (2025) [1]	Blockchain in healthcare (survey)	Yes	No	No	Yes	No	No	No consent lifecycle or revocation
This review	Blockchain + dynamic consent for secondary use	Yes	Yes	Yes	Yes	Yes	Yes	End-to-end lifecycle, revocation propagation, auditability, EHDS focus

Scope and Contribution of the Review

The purpose of this review is to deliver a thorough and systematic examination of blockchain-based frameworks that will support dynamic, auditable, and revocable consent for the secondary use of health data. It adds to current studies by investigating how these systems will manage the full life cycle of consent in healthcare using blockchain and decentralized identity technologies. It also evaluates the system's technical reliability, usability, and compliance with regulatory standards. In bringing these findings together, this review highlights common design approaches and enduring challenges across these separate studies. By integrating findings from technological, ethical, and governance perspectives, it explains how blockchain can enable patient-centric consent systems. It also makes practical recommendations for researchers, system developers, healthcare providers, and policymakers.

More specifically, this review makes four key contributions. First, it provides a PRISMA 2020–compliant synthesis of recent literature published between 2020 and 2025, focusing explicitly on blockchain-enabled dynamic and revocable consent for the secondary use of health data. Second, it applies a multi-dimensional analytical framework encompassing consent lifecycle management, auditability, usability, and legal–ethical alignment, complemented by a structured quality assessment of the included studies. Third, it identifies recurring architectural patterns such as hybrid on-chain/off-chain designs and the use of decentralized identifiers (DIDs) and verifiable credentials (VCs) and analyses their implications for interoperability, revocation enforcement, and compliance with GDPR and the emerging European Health Data Space (EHDS) framework. Finally, it highlights critical gaps and future research directions required to advance these systems from conceptual prototypes toward operational healthcare infrastructures.

Objectives and Aims of the Review

The aim of this systematic review is to synthesize and critically evaluate blockchain-based frameworks that support dynamic, auditable, and revocable consent for the secondary use of health data. Specifically, the review seeks to (1) characterize the architectural and operational approaches used to model and enforce consent lifecycles; (2) assess how auditability, provenance, and accountability are implemented across distributed systems; and (3) evaluate the extent to which proposed solutions address usability, interoperability, and regulatory alignment, including compliance with the GDPR and the emerging European Health Data Space (EHDS).

Together, these objectives frame the review's analytical focus on both technical maturity and practical readiness for real-world deployment.

Methods

This systematic review was conducted to identify, analyze, and synthesize peer-reviewed literatures on blockchain-based frameworks that enable dynamic, auditable, and revocable consent for the secondary use of health data. The review followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure transparency and reproducibility. The methodological steps included defining eligibility criteria, developing a comprehensive search strategy, screening and selecting studies, extracting and synthesizing data, performing a structured quality assessment and classifying findings according to a conceptual analytical framework.

Review Design

A systematic literature review approach was selected to provide a comprehensive and structured overview of the current research landscape. This design supports evidence-based synthesis by integrating findings from diverse studies that address similar research questions across technical, ethical, and regulatory dimensions. The review focused on primary research papers, system proposals, prototypes, and evaluations that describe blockchain-based consent management models relevant to healthcare data reuse. Conceptual papers were included only if they contributed a defined architectural or governance model. The review protocol was defined in advance to minimize selection bias and ensure consistency across screening, data extraction, and synthesis phases.

Eligibility Criteria

Eligibility criteria were established using the PICOS (Population, Intervention, Comparison, Outcome, and Study type) framework, which ensures a consistent and unbiased selection process.

Inclusion criteria for this research includes:

- Studies proposing or evaluating blockchain or distributed-ledger–based consent systems within healthcare contexts.
- Systems explicitly supporting dynamic consent, including granular, time-bound, or revocable authorization.
- Studies addressing secondary use of health data, such as in research, AI model development, clinical trials, or data analytics.
- Peer-reviewed journal publications between January 2020 and October 2025**.**
- Publications written in English.

To improve clarity and reproducibility, the inclusion criteria were operationalized as follows:

(i) Population: healthcare stakeholders and patient data contexts;
(ii) Intervention: blockchain/DLT-based consent management mechanisms;
(iii) Comparison: not mandatory, as most studies proposed novel frameworks;
(iv) Outcomes: support for dynamic, auditable, and revocable consent and/or reported technical or usability evaluation; and
(v) Study type: peer-reviewed empirical, prototype, or architectural studies.

Likewise, the research was set with the following exclusion criteria to filter out the irrelevant articles:

- Studies unrelated to healthcare or consent management.
- Solutions limited to static, one-time consent without revocation or modification features.
- Opinion pieces, editorials, or commentaries without technical or empirical contribution.
- Duplicates or non-peer-reviewed materials such as white papers and thesis or dissertations.

- Conference papers were excluded unless extended journal versions were available, in order to ensure sufficient methodological detail and maturity of the included studies.

Information Sources and Search Strategy

The literature search was performed across three major electronic databases known for health informatics and blockchain research: PubMed, Scopus and Web of Science. A Boolean search string was developed and adapted to each database's syntax, combining key terms related to consent management, blockchain, and health data reuse. The core search expression used was:

("dynamic consent" OR "revocable consent" OR "granular consent") AND
("blockchain" OR "distributed ledger" OR "DLT") AND
("health" OR "healthcare" OR "medical data") AND
("secondary use" OR "research" OR "data sharing" OR "AI training")

The core Boolean search strategy was adapted to the syntax and indexing mechanisms of each database. In PubMed, the search was applied to title and abstract fields and supplemented with relevant Medical Subject Headings (MeSH) where available. In Scopus and Web of Science, the search was executed using title, abstract, and keyword fields, with database-specific field tags and operators applied to preserve semantic equivalence across platforms. Truncation and phrase matching were used where supported. These adaptations ensured comprehensive retrieval while maintaining consistency in search intent across databases. The complete database-specific query formulations are available from the authors upon request to support reproducibility.

The final searches were conducted in October 2025, and the results were limited to publications between January 2020 and October 2025. Search fields included titles, abstracts, and keywords where supported by the databases.

Reference lists of included studies were manually screened to identify additional relevant publications not captured by database queries. All records retrieved from the search were exported to a Zotero citation manager [23] for de-duplication and structured screening. The complete search strategy and database-specific query adaptations are available upon request to support reproducibility.

Study Selection Process

The selection process was conducted in two main stages:

- Title and Abstract Screening: Each record was independently reviewed to assess relevance against inclusion criteria. Articles clearly outside the healthcare or blockchain domain were excluded at this stage.
- Full-Text Review: Potentially relevant studies were examined in full to confirm eligibility and to ensure that they met the review's focus on dynamic and revocable consent mechanisms.

Any discrepancies in inclusion decisions were resolved by discussion among authors to reach consensus. The entire process was documented using a PRISMA 2020 flow diagram, which summarizes the number of records identified, screened, excluded, and included in the final analysis.

Specifically, two authors SP and MB independently screened all titles and abstracts, and disagreements were resolved through discussion, consulted with the authors RB and JCF when consensus could not be reached. The same procedure was applied during full-text assessment.

Inter-rater agreement between the two reviewers was assessed to evaluate screening consistency. Agreement was substantial, with a Cohen's kappa coefficient of $\kappa = 0.78$ during title and abstract screening and $\kappa = 0.81$ during full-text eligibility assessment, indicating a high level of concordance. Discrepancies were resolved through discussion and, where necessary, consultation with senior authors to reach consensus.

Data Extraction and Coding

A standardized data extraction form was designed to ensure consistency in collecting relevant details from each study. The following key attributes were extracted:

- Bibliographic details: authors, publication year, source, and country of origin.
- Use case: healthcare domain, population, and purpose of data sharing.
- Blockchain architecture: platform, consensus model, and smart contract use.
- Identity management: use of DIDs, VCs, or public key infrastructure.
- Consent features: lifecycle stages supported (grant, modify, revoke), granularity, and enforcement mechanisms.
- Auditability mechanisms: on-chain logging, event tracking, hash anchoring, or hybrid verification models.
- Usability aspects: interface design, patient engagement, and evaluation methods.
- Compliance and ethics: references to GDPR, EHDS, or ethical principles.
- Reported challenges**:** technical, organizational, or legal barriers to implementation.

Additional fields were included to capture blockchain deployment models (public, permissioned, or consortium), hybrid on-chain/off-chain designs, and any mechanisms for automated revocation propagation or integration with clinical systems (e.g., HL7 FHIR).

Extracted data were entered into a structured spreadsheet and cross-verified for accuracy and completeness. Data extraction was performed independently by two reviewers on a subset of studies to validate consistency, with disagreements resolved through discussion.

Analytical Framework and Data Synthesis

The synthesis process combined quantitative description with qualitative thematic analysis to identify design patterns and conceptual trends across studies. The analysis was guided by four key conceptual dimensions derived from the literature and regulatory frameworks:

i. Consent Lifecycle Management: How systems model, enforce, and update consent states, including mechanisms for revocation.
ii. Auditability and Traceability: The extent to which systems provide immutable and verifiable records of consent and data access.
iii. Usability and Patient Empowerment: The user-facing design and degree of patient control supported by interfaces or wallets.
iv. Legal and Ethical Alignment: Compliance with data protection laws and ethical requirements related to transparency, purpose limitation, and revocability.

Studies were coded against these dimensions and grouped into thematic clusters to highlight common technical approaches, gaps, and best practices. Where relevant, architectural diagrams and comparative tables were used to illustrate design similarities and differences.

Quantitative findings, such as the prevalence of blockchain platforms or identity mechanisms, were summarized using descriptive statistics, while qualitative findings were narratively synthesized to contextualize patterns and highlight challenges. The combined synthesis enabled cross-dimensional analysis, for example linking architectural choices to observed usability or compliance limitations.

Quality Assessment

To ensure methodological rigor, each included study was evaluated for quality using a set of predefined criteria adapted from digital-health and software-engineering review frameworks. These criteria assessed:

- Clarity of objectives and problem definition.
- Transparency in describing the system's architecture or implementation.
- Explicit discussion of consent mechanisms and revocation of support.
- Alignment with privacy or regulatory standards.
- Evidence of validation, testing, or pilot evaluation.

Each criterion was scored as 0 (not met), 0.5 (partially met), or 1 (fully met). Scores were summed and normalized to a 0–1 scale to derive an overall Quality Index (QI) score for each study. All criteria were equally weighted, as the review aimed to balance architectural transparency, consent lifecycle enforceability, regulatory alignment, and empirical maturity. While no studies were excluded solely based on quality, the assessment was used to weight the interpretation of results, identify recurring methodological limitations, and contextualize the strength of the evidence base. Quality assessment was performed independently by the authors SP and MB on all included studies, with disagreements resolved through a collective discussion to ensure consistency.

Aggregate quality trends were later analyzed to distinguish between conceptual proposals and empirically validated implementations, and to support sensitivity analysis in the synthesis of results.

As part of this sensitivity analysis, findings were re-examined by restricting the synthesis to studies with QI ≥ 0.75. This analysis showed that while high-level architectural patterns (eg, hybrid on-chain/off-chain designs and smart contract–based consent modelling) remained consistent, claims related to automated revocation propagation, usability validation, and enforcement assurance were supported by only a small subset of higher-quality studies. No study reported quantitative latency or completeness guarantees for revocation enforcement across distributed data custodians.

Results

This section presents the findings of the systematic review based on the analysis of 55 peer-reviewed studies that explore blockchain-based consent management frameworks for healthcare data sharing and secondary data use. The results are structured following the PRISMA process and analyzed according to the four conceptual dimensions defined earlier, consent lifecycle management, auditability and traceability, usability and patient empowerment, and legal and ethical alignment.

Conceptual Overview

Before presenting the results of the systematic analysis, Figure 1 illustrates a generalized conceptual architecture reflecting the most common consent workflow patterns identified across the reviewed studies. The model summarizes how blockchain-based infrastructures support consent granting, verification, revocation, and audit logging for the secondary use of health data, and serves as a reference architecture for the subsequent thematic analysis.

This conceptual model is not derived from a single implementation but represents an abstraction of recurring architectural elements observed across the literature, including hybrid on-chain/off-chain designs, smart contract–based consent logic, decentralized identifiers, and off-chain policy enforcement components. In line with the majority of reviewed frameworks, the model assumes a permissioned or consortium blockchain environment, in which participating healthcare and research institutions operate trusted nodes under defined governance and access-control policies.

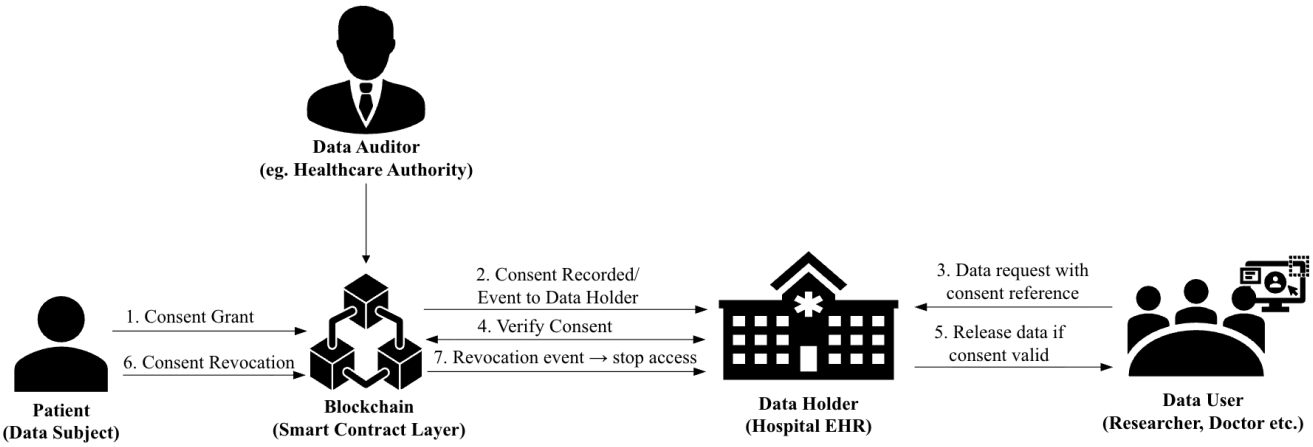


Figure 1: Conceptual architecture of blockchain-based consent management for secondary use of health data

As shown in Figure 1, the consent workflow proceeds through the following steps.
Step 1 begins when the data subject grants consent through a patient-facing application or digital identity wallet. This consent action is submitted to the blockchain via a smart contract, which records the consent state immutably on-chain.
Step 2 propagates the consent creation or update event from the blockchain to the data holder, enabling synchronization of local access-control and enforcement mechanisms.
Step 3 occurs when a data requester submits a request for secondary use of health data, including a reference to the relevant consent identifier.
Step 4 represents a bidirectional interaction between the data requester or data holder and the blockchain, in which the smart contract verifies the current consent state and returns an acknowledgment indicating whether access conditions are satisfied.
Step 5 allows the data holder to release the requested data, if consent has been verified and all access conditions are met. Sensitive health data remain off-chain throughout this process and are accessed only through controlled institutional interfaces.
Step 6 enables the data subject to revoke previously granted consent, with the revocation recorded on-chain through a smart contract transaction.
Step 7 disseminates the revocation event to subscribed data holders, ensuring that local enforcement mechanisms are promptly updated and that subsequent access requests are denied in accordance with the updated consent state.
Although the blockchain serves as the authoritative record of consent, data holders maintain a synchronized local enforcement state to support low-latency access control, auditing, and operational continuity. This local state is derived from on-chain consent events (Steps 2 and 7) and does not replace blockchain-based verification.
Overall, blockchain functions primarily as a coordination and audit layer, anchoring consent events and access proofs rather than storing personal health data. This baseline hybrid architecture underpins the subsequent analysis of consent lifecycle management, auditability, usability, and legal–ethical alignment across the reviewed studies.

Study Selection

The comprehensive search across three academic databases (PubMed, Scopus and Web of Science) initially yielded 205 records. After duplicate removal and screening for relevance, 55 studies met all inclusion criteria.
The included studies were published between 2020 and 2025, indicating that blockchain-enabled consent management is a relatively recent and rapidly expanding area of research. The number of publications peaked in 2023, reflecting growing maturity and convergence of blockchain and healthcare data-sharing technologies. Figure 2, shows the publication trend of the articles across the years.

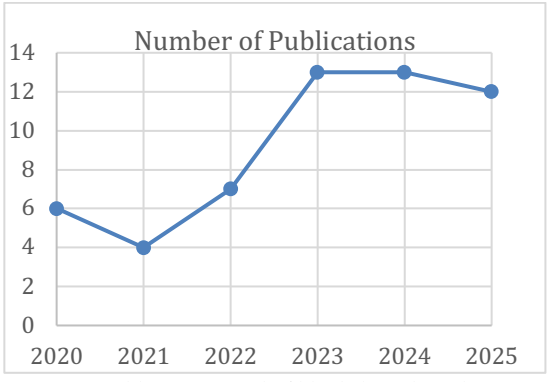


Figure 2: Publication trend of blockchain-based consent management studies (2020-2025)

The PRISMA 2020 flow diagram presented in **Error! Reference source not found.** illustrates the identification, screening, eligibility assessment and final inclusion of studies, while a detailed summary of all included studies is provided in Table 2.
Specifically, 205 records were identified through database searching. After removal of 20 duplicates, 185 records were screened by title and abstract, of which 94 were excluded. Ninety-one full-text articles were sought for retrieval, 11 could not be accessed, and 80 reports were assessed for eligibility. Of these, 25 were excluded for not meeting the inclusion criteria, resulting in 55 studies included in the final synthesis.

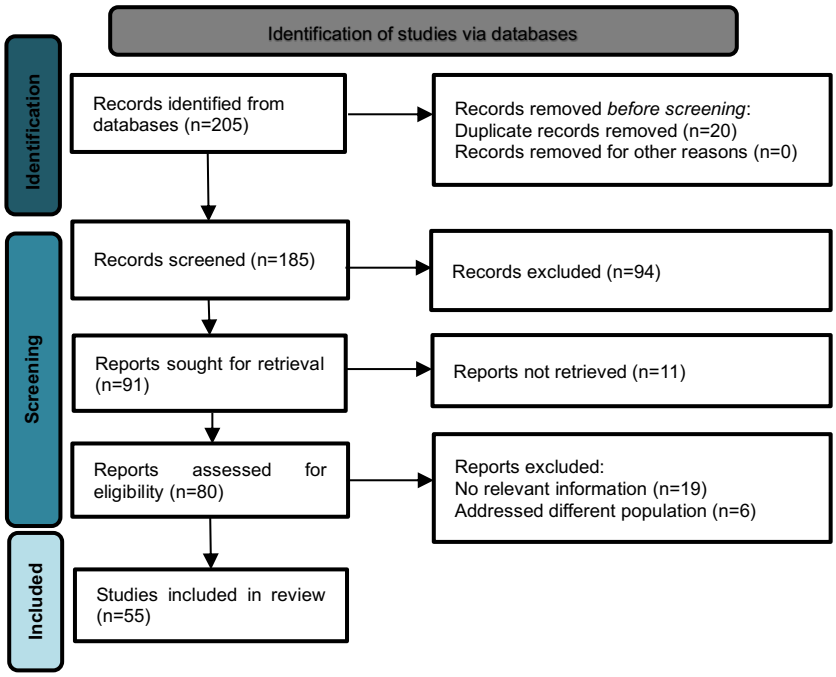


Figure 3: PRISMA Workflow

Descriptive Summary of Included Studies

Among the 55 papers, 43 (78%) explicitly implemented or proposed blockchain-based consent management frameworks, and 39 out of 55 studies (71%) incorporated features of dynamic or revocable consent. 52 out of 55 studies (95%) addressed healthcare data-sharing scenarios, and every study (55) engaged with data security and privacy considerations.
Figure 4 presents a high-level thematic classification of the reviewed studies based on their primary analytical focus. Although several studies address multiple themes (as reflected in Table 2), each paper was assigned to one dominant category for the purpose of visual aggregation. The dominant category was determined based on the main contribution emphasized in the study's objectives, system design, and evaluation. While Figure 4 shows a single dominant classification per study for visualization purposes, Table 2 provides a multi-label thematic mapping, allowing studies to be associated with multiple categories. In Figure 4, the category 'Blockchain' refers to studies whose primary contribution lies in the design or analysis of blockchain-based systems or infrastructures, rather than in consent mechanisms or application-level workflows.

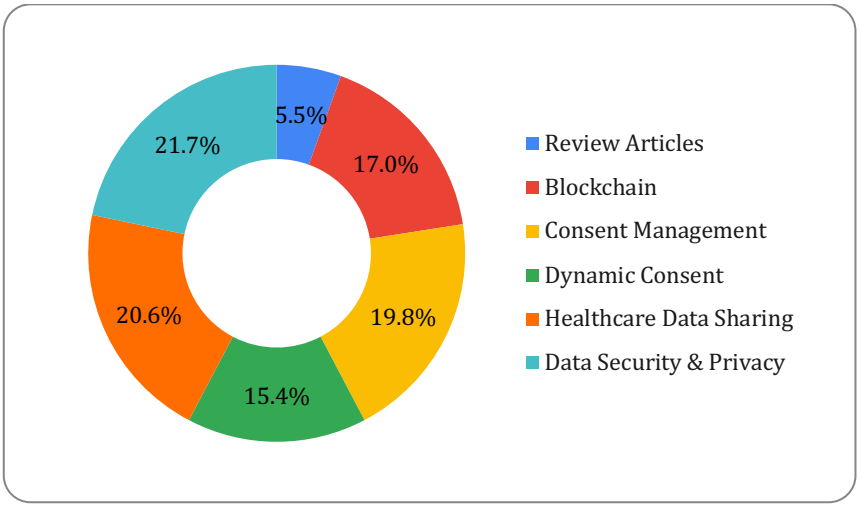


Figure 4: Primary thematic classification of reviewed studies

In terms of domain focus, clinical trials accounted for the largest application area, followed by personal health records (PHRs) and digital-health research environments. Fewer studies focused on biomedical research governance, genomic data-sharing, or cross-institutional interoperability pilots.

Table 2 summarizes the quantitative characteristics of the included studies. The majority of works were published between 2022 and 2024, reflecting the rapid growth of interest in blockchain-enabled consent management. Ethereum and Hyperledger Fabric were the most frequently used blockchain platforms, while Quorum and Polygon appeared in several experimental prototypes, where the majority of reviewed systems were deployed on permissioned or consortium blockchains, reflecting governance and access-control requirements in regulated healthcare environments.

Table 2. Overview of quantitative characteristics of included studies

Category	Dominant Themes / Counts
Total studies included	55
Year range	2020 - 2025
Most active publication year	2023 - 2024
Blockchain-based systems	43
Dynamic or revocable consent	39
Healthcare-related applications	52
Privacy or security addressed	55
Leading application areas	Clinical trials, PHRs, digital-health research

Influence of Application Domain, Platform Choice, and System Maturity

The reviewed studies exhibited substantial heterogeneity in application domain, blockchain platform, and implementation maturity, which influenced the nature and strength of reported findings. Studies focused on clinical trials and biomedical research more frequently implemented dynamic consent and auditability mechanisms, reflecting established governance requirements and sponsor accountability. In contrast, frameworks targeting EHRs and health information exchange more often emphasized access control and interoperability but provided less detail on consent lifecycle enforcement.

Platform choice also affected system design. Permissioned and consortium blockchains, particularly Hyperledger Fabric, were predominantly used in healthcare-specific deployments and pilot studies, enabling finer governance control and alignment with regulatory requirements. Public blockchain–based proposals, often built on Ethereum, were more common in conceptual or proof-of-concept studies and tended to focus on smart contract expressiveness rather than operational compliance.

Finally, implementation maturity strongly shaped reported outcomes. Conceptual and prototype-level studies frequently claimed support for revocation and patient empowerment, whereas deployed or pilot systems more often reported constraints related to latency, institutional integration, and usability. As a result, higher-maturity implementations demonstrated narrower but more realistic functionality, while lower-maturity studies reported broader capabilities with limited empirical validation.

Thematic Classification

The selected studies were systematically analyzed according to the four conceptual dimensions defined in the analytical framework: (i) Consent Lifecycle Management, (ii) Auditability and Traceability, (iii) Usability and Patient Empowerment, and (iv) Legal and Ethical Alignment. This thematic synthesis reveals both the convergence of design strategies across studies and the heterogeneity in their technical maturity, regulatory focus, and evaluation depth.

Consent Lifecycle Management

Across the dataset, most frameworks supported dynamic consent flows allowing users to grant, modify, and revoke consent at multiple stages of data sharing. Smart contracts were widely used to represent consent states, recording events such as *ConsentGranted*, *ConsentUpdated*, and *ConsentRevoked,* which represent the consent states as the programmable states within the smart contracts and, they are automatically triggered based on predefined conditions. Dynamic and revocable consent was the most frequently addressed theme across the dataset. Approximately two-thirds of the selected papers implemented explicit revocation mechanisms**,** with 35 out of 55 studies (64%) distinguishing between active revocation (initiated by the data subject) and 6 out of 55 papers (11%) adopting time-based or condition-based revocation (automatically triggered by contract logic). However, only a 3 out of 55 of the studies (5%) relied on administrator-initiated withdrawal.

To provide an overview of how consent lifecycle management is addressed across the literature, Table 3 summarizes the studies that explicitly support dynamic consent features, including mechanisms for granting, modifying, and revoking consent. The table highlights the diversity of application domains and technical approaches through which lifecycle control is operationalized in blockchain-enabled frameworks.

Table 3. Studies addressing consent lifecycle management

Authors & Date	Major Contribution	Application Area
Kim et al. (2022) [24]	Mobile PHR app with dynamic consent history (SUS validated)	Personal Health Records (PHR)
Alhajri et al. (2022) [25]	Decentralized GDPR-compliant consent via smart contracts	Wearable Fitness Data / Healthcare
Albalwy et al. (2021) [5]	Designed ConsentChain enabling patients to dynamically grant/ withdraw consent for genomic data sharing; ontology-based automation of consent.	Clinical Genomic Data Sharing
Can et al. (2024) [20]	Proposed hybrid architecture with a “purpose tree” for consent management	General GDPR Consent Management
Dong et al. (2023) [26]	Built BEST platform with patient-controlled consent	Personal Health Records (PHR)

Jaiman & Urovi (2020) [27]	Created a dynamic consent model with DUO + ADA-M ontologies, machine-readable consent and revocation for health data.	General Health Data Sharing
Peyrone & Wichadakul (2023) [28]	Supported consent withdrawal, renewal, audit logs	General Data Sharing
Daudén-Esmel et al. (2024) [29]	Proposed a blockchain-based access control system for healthcare consent management	Healthcare Consent & Access Control
Charles et al. (2024) [19]	Presented blockchain-based dynamic consent model for patient-centric research, clinical trials, and health informatics	Patient-Centric Research / Clinical Trials
Roman-Martinez et al. (2023) [30]	Proposed service-oriented blockchain architecture integrating consent management	Healthcare Data Sharing / Consent Mgmt
Kim et al. (2021) [31]	Built a patient-consent blockchain platform (PHR) using Hyperledger Fabric with on/off-chain data storage	Personal Health Records
Mishra & Mehra (2025) [32]	Proposed DiabeticChain, a blockchain framework for patient-controlled diabetes data sharing	Diabetes / Chronic Disease Management
Pham et al. (2024) [33]	Demonstrated feasibility of informed consent system for multi-site clinical research dynamic consent handling across thousands of records.	Clinical Research
Albanese et al. (2020) [15]	Proposed a private blockchain architecture to manage dynamic consent in clinical trials	Clinical Trials
Muller et al. (2023) [14]	Survey-based study showing patients prefer dynamic consent and continuous communication in large-scale data reuse	Large-Scale Health Data Reuse
Dankar et al. (2020) [34]	Introduced dynamic informed consent for large-scale genomics; proposed dynamic consent as a solution for transparency and patient control.	Genomics / Population Sequencing
Kim et al. (2021) [35]	Designed Dynamichain, integrating dynamic consent for medical data sharing	Healthcare Data Ecosystem
Barnes et al. (2025) [36]	Introduced "demonstrated consent": a hybrid model combining blockchain (NFTs tied to samples) and generative AI (LLMs) for interactive, transparent communication in biobanking.	Biobanking
Khalid et al. (2023) [37]	Proposed a formal security model for Dynamic Consent Management System	Dynamic Consent in e-Healthcare
Huh et al. (2022) [38]	Patient engagement with blockchain-enabled dynamic consent	Clinical Trials
Despotou et al. (2020) [39]	Surveyed patient attitudes on blockchain-based digital consent for dynamic health data sharing	Digital Health / Patient Perception
Lee et al. (2023) [40]	Empirical study identifying organizational, technical, and social factors that promote or hinder adoption of dynamic consent in digital health ecosystems.	Digital Health
Tith et al. (2020) [41]	Developed purpose-based access control model for patient consent	EHRs / Biobanking
Khalid et al. (2023) [42]	Proposed decentralized privacy-first Dynamic Consent Management System with patient empowerment	e-Healthcare
Singh & Rathee (2025) [43]	Developed a smart contract–based dynamic consent model integrating decentralized storage (IPFS) and fine-grained access control for healthcare data.	Healthcare Applications
Rohini et al. (2024) [44]	Introduced a blockchain-based consent model for Health Information Exchange (HIE)	Health Information Exchange
Lee & Lee (2022) [18]	Dynamic consent in IoT healthcare	Healthcare IoT
Castro et al. (2024) [45]	Identifies patient consent management as a core application of blockchain in clinical trials, highlighting smart contracts for automating electronic and dynamic consent	Blockchain-enabled consent management
Gondode et al. (2025) [46]	Highlights blockchain-based management of patient consent and advance directives in critical care, using immutable records and smart contracts	Patient Consent and ICU and Emergency Care
Gupta et al. (2024) [47]	Highlights blockchain-based informed consent in clinical trials as a critical use case, emphasizing smart contracts for recording, re-consenting after protocol changes	Blockchain-enabled dynamic consent management
Kasyapa & Vanmathi (2024) [48]	Blockchain-based patient control and consent mechanisms using smart contracts, emphasizing secure authorization, patient ownership of EHRs, automated access control, and dynamic consent handling	Patient-centric consent and access control
Nguyen et al. (2025) [49]	Proposes a dual-blockchain ecosystem that enables fine-grained, segment-level access control over DNA sequences, allowing patients to dynamically assign, update, and revoke permissions	Dynamic consent and access control
Righi et al. (2025) [50]	Incorporates GDPR/LGPD-compliant informed consent within edge controllers, allowing citizens to subscribe to health services, select which vital signs to share, define data usage purposes, and revoke participation by deleting accounts, supporting user-controlled and dynamic consent in large-scale monitoring systems	User-driven consent and access control
Felemban et al. (2025) [51]	Highlights blockchain-enabled dynamic and surgical consent models, proposing decentralized, timestamped, and patient-accessible consent records	Dynamic informed consent for surgery
Hovorushchenko et al. (2023) [22]	Physicians request access through validators and custodians, supporting consent-driven authorization, role-based access, and controlled release of medical data using smart-contract–like workflows	Consent-aware sharing of electronic medical data

To examine revocation propagation mechanisms in greater depth, Table 4 presents a focused analysis of representative frameworks, detailing their propagation mechanisms, enforcement layers, operational scope, and evaluation evidence.

Table 4. Revocation propagation: mechanism, scope, and evidence.

Study	Propagation mechanism	Enforcement layer	Scope	Evaluation	Latency / assurance reported	Notes
DynamiChain (Kim et al., 2021) [35]	NR (conceptual time-bound expiry; no explicit listener/API described)	On-chain check (time-stamp validation)	NR (likely single site / conceptual)	Sim/Lab (conceptual prototype)	Not reported	Implements consent expiry via timestamps; propagation beyond a single relying party appears conceptual only.
BEST (Dong et al., 2023) [26]	Event listener/API integration to off-chain access control (described)	Hybrid (blockchain audit + off-chain PDP/PEP)	Single site (NR for cross-institution)	Lab prototype	Not reported	Demonstrates synchronisation between ledger events and PHR sharing controllers; no explicit latency benchmarks.
METORY (Huh et al., 2022) [52]	Event listener/API (NR for exact pattern)	Hybrid (smart-contract status + site controllers)	Multi-site (clinical trial settings)	Pilot (multicenter)	Not reported	Operational deployment in multicenter trials; improved transparency/retention reported; no latency numbers.
Roman-Martinez et al., 2023 [30]	Service orchestration / API gateway (conceptual)	Hybrid (on-chain state + off-chain services)	Cross-institution (conceptual)	Conceptual / Lab	Not reported	Architecture-level description; propagation pathways proposed but not benchmarked (conceptual only).
Can et al., 2024 [20]	Event listeners/APIs (described; implementation depth NR)	Hybrid (auditable consent with on/off-chain)	Multi-site (NR for real deployment)	Lab / Prototype	Not reported	Hybrid auditable consent; propagation discussed; evidence suggests prototype-level implementation without latency metrics.

For example, DynamiChain [35] enabled real-time consent expiry via timestamp validation, and the works presented by [5,33,41] also used Solidity contracts to encode purpose-specific permissions and time-bound access. While some other works such as [26,35] represented consent through chaincode with endorsement policies ensuring institutional accountability. The works such as METORY [52] and BEST [26] demonstrated practical synchronization between blockchain and off-chain access-control layers. While few works like [20,30] explored how consent withdrawal could automatically cascaded to all data custodians through event listeners or APIs. Overall, most studies successfully demonstrated programmable consent logic at a conceptual or prototype level, but large-scale validation in production environments remained limited.

Only 5 of the 55 reviewed studies (9%) described any mechanism intended to propagate consent revocation beyond the blockchain layer. Among these, only 3 studies (5%) implemented or evaluated such propagation beyond a purely conceptual design. None quantified propagation latency. After sensitivity analysis (QI ≥ 0.75), this reduced to 0 studies, underscoring the critical gap in real-world implementation of revocable consent (Table IV).

Beyond the low prevalence of revocation propagation mechanisms, the reviewed studies provide limited insight into the underlying reasons for this gap. Across the literature, revocation is typically modelled as a smart-contract state transition, while downstream enforcement across distributed off-chain systems is left implicit. This suggests unresolved technical challenges in synchronizing on-chain consent states with heterogeneous institutional policy enforcement points. In addition, regulatory uncertainty regarding the interpretation of "logical deletion" under GDPR Article 17, combined with the absence of performance benchmarks and certification incentives, appears to discourage implementation beyond proof-of-concept designs.

Auditability and Traceability

Auditability was one of the most consistent themes across the corpus. Blockchain's immutability and append-only structure make it a natural foundation for verifiable audit trails. Among the reviewed studies, 27 out of 55 studies **(**49%) leveraged blockchain's immutable ledger to maintain verifiable audit trails of consent and data-access events, as summarized in Table 5.

Three dominant audit models emerged:

1. On-chain logging**,** where all consent transactions are recorded directly on the ledger for maximum transparency.
2. Hybrid anchoring**,** where detailed logs are stored off-chain but cryptographically hashed and referenced on-chain.
3. Smart-contract state verification**,** where consent status is query able through verifiable contract variables.

While these models enhance transparency, several studies noted that blockchain audit logs remain technically complex and not easily interpretable by patients or regulators**.** Only a small subset provided visual audit dashboards or user-readable verification tools, such as the works presented in METORY [52], BEST [26] and SmartDataTrust [28], which provided graphical summaries of consent events. However, most systems exposed raw transaction logs or hashes which are not easily interpretable by patients or auditors. This indicates that technical auditability does not always translate to practical accountability**.**

A small subset, 7 out of 55 studies (13%) such as [30,44] implemented FHIR AuditEvent resources to bridge blockchain logs with clinical systems. Some recent works like [42] are experimenting with zero-knowledge proofs to verify data access without revealing identifiers, which preserves the privacy of data accessors while exposing only the minimum information required for audit and compliance.

Table 5. Studies focusing on auditability and traceability

Authors & Date	Audit/Trace Contribution	Application Area
al. (2024) [20]	l architecture with consent management and introduced auditing mechanisms	nt Management
t al. (2023) [26]	able logs in the proposed BEST platform	al Health Records (PHR)
ıe & Wichadakul (2023)	rted consent withdrawal, renewal and audit logs	al Healthcare Data Sharing
t al. (2022) [6]	ehensive survey of blockchain in clinical trials, consent traceability, monitori anagement	al Trials
et al. (2023) [7]	cted multivocal literature review mapping blockchain applications in healthca	al Health Domain
et al. (2022) [53]	ed a blockchain-based privacy-preserving data governance framework ensuri itability, transparency, and compliance across multiple stakeholders	Stakeholder Data Governance
n-Esmel et al. (2024) [2	ed a blockchain-based access control system for healthcare consent managem sized efficiency, scalability, and secure patient-controlled access to medical s	care Consent & Access Control
ı-Martinez et al. (2023) [	ed blockchain architecture integrating consent management, access control, a g for compliance and interoperability	care Data Sharing / Consent Mgmt
al. (2023) [54]	ed a hybrid blockchain–deep learning architecture for secure and scalable care data management	al Healthcare Systems
al. (2021) [31]	patient-consent blockchain platform (PHR) using Hyperledger Fabric with chain data storage; Immutable PHR logs	al Health Records
t al. (2024) [33]	ıstrated feasibility of Immutability in access logs	al Research
se et al. (2020) [15]	bility in clinical trials	al Trials
al. (2021) [35]	ıed Dynamichain, a blockchain-based healthcare ecosystem integrating dynam t for medical data sharing; demonstrated system architecture and use cases.	care Data Ecosystem
ushchenko et al. (2023) [	ved blockchain-based approaches for medical data management; proposed ication of methods, highlighting challenges in scalability, privacy, and erability.	al Healthcare Data Mgmt
al. (2022) [52]	ıed METORY platform, a blockchain-based DCMS tailored for clinical trials, ting dynamic consent updates, secure auditability, and decentralized governar	al Trials
al. (2020) [41]	oped purpose-based access control model for patient consent, implemented edger fabric audit trials	/ Biobanking
t et al. (2023) [55]	ed a framework for securing off-chain data storage in blockchain-based conse ıs	care Data Sharing / Off-chain Storage
et al. (2024) [44]	ıced a blockchain-based immutable logging	Information Exchange
et al. (2024) [45]	ıstrates blockchain's role in enhancing transparency, data integrity, traceability ucibility of clinical trial data	arent and auditable clinical trial
de et al. (2025) [46]	how blockchain enables tamper-proof EHRs, immutable audit trails, ırent data sharing in ICUs	ible EHR management
et al. (2024) [47]	sizes cross-industry evidence showing blockchain's role in enabling immu rails and end-to-end traceability	ible supply chain management
oa & Vanmathi (2024) [4	ıatically synthesizes how blockchain enables immutable audit trails, data inte d-to-end traceability across healthcare use cases	ible EHR systems
& In (2024) [56]	zes how blockchain-integrated decentralized storage ensures immutable rec ble data transactions, cryptographic integrity	ible decentralized storage
n et al. (2025) [49]	ıstrates how immutable ledgers and encrypted on-chain access tickets pr -proof audit trails	ible genomic data sharing
t et al. (2025) [50]	es a hierarchical edge–fog–cloud architecture with data traceability ser ıg-based storage, and immutable logging of vital-sign data paths	ible remote health monitoring
oan et al. (2025) [51]	sizes current and emerging uses of blockchain for immutable audit trails ıility in healthcare	ible EHR systems
ushchenko et al. (2023) [	es blockchain-based methods for medical data management that ensure immu e, provenance, and tamper-proof audit trail	ible EHR management

Usability and Patient Empowerment

Usability remains a significant bottleneck in real-world adoption and findings in this literature study were also mixed. Many systems incorporated patient-facing interfaces or portals that allowed individuals to view and adjust consent preferences. Altogether 19 out of 55 studies (35%) proposed some form of user interface for managing consent, yet only 11 out of 55 studies (20%) conducted formal usability or acceptance testing, as summarized in Table 6. Most systems targeted patients via mobile or web dashboards, but interactions often required manual cryptographic signing or wallet operations beyond typical health literacy levels. About one-third of the studies integrated decentralized-identity wallets supporting DIDs and VCs to give users more direct control. Technical interactions, such as cryptographic signing and blockchain transactions, were often found to be too complex for typical patients. Where formal usability studies were conducted, results showed improved trust and willingness to share data when transparency and visual feedback mechanisms were present. Overall, patient empowerment was widely emphasized but poorly operationalized, revealing a significant gap between conceptual ideals and deployable user experiences.

Out of the studied articles, the mobile PHR app presented by Kim et al. [24] achieved a SUS score of 74, while [57] co-designed the "de-bi", biobanking app with patients, which resulted in enhanced trust and engagement and the METORY platform by [52] was found to have increased transparency and participant retention in multicenter trials.
Furthermore, 18 out of 55 studies (33%) integrated DID or VC mechanisms for self-sovereign consent representation [19,42]. These frameworks aligned with emerging EUDI Wallet specifications to enable portable, user-controlled consent tokens. Only a few works addressed multi-language interfaces, visual consent explainers or voice assistants features vital for inclusive health data governance. Studies that did incorporate co-design or participatory approaches [39,57] reported higher user trust and perceived autonomy. Collectively, while patient empowerment is a recurrent objective, the translation of this principle into intuitive design remains emerging. Human-centered and iterative design methods remain underutilized in this domain.

Table 6. Studies emphasizing usability & patient empowerment

Authors & Date	Usability/Empowerment Focus	Application Area
: al. (2022) [24]	ɔped and tested a blockchain-applied mobile PHR app with usability validation (SU ity Scale (SUS) score 74.0	ıal Health Records (PHR)
s et al. (2024) [19]	ıted blockchain-based dynamic consent model for patient-centric research, clinical trials informatics applications.	t-Centric Research / Clinical Trial
ı et al. (2025) [57]	signed a decentralized mobile app ("de-bi") with breast cancer patients, enal arency and engagement in biobank specimen use.	ıking / Patient Engagement
dt et al. (2025) [8]	ıg review mapping technical implementations of informed consent in digital health; ident ıges (obtain, prove, retrace, manage)	l Health / mHealth Consent
: al. (2021) [31]	ledger Fabric with on/off-chain data storage; empowered patients with ownership of P ıic consent, and secure sharing across hospitals.	ıal Health Records
ı & Mehra (2025) [3	ed DiabeticChain, a blockchain framework for patient-controlled diabetes data sharing	es / Chronic Disease Managemen
et al. (2023) [14]	/-based study showing patients prefer dynamic consent and continuous communicati scale data reuse; emphasized patient-centric governance.	Scale Health Data Reuse
r et al. (2020) [34]	ghted ethical challenges in sequencing and proposed dynamic consent as a solutio arency and patient control.	ıics / Population Sequencing
: et al. (2025) [36]	uced "demonstrated consent": a hybrid model combining blockchain (NFTs tied to sam nerative AI (LLMs) for interactive, transparent communication in biobanking.	ıking
tou et al. (2020) [39	ved patient attitudes on blockchain-based digital consent for dynamic health data sha patients valued transparency, control, and security.	l Health / Patient Perception
al. (2023) [40]	ical study identifying organizational, technical, and social factors that promote or h on of dynamic consent in digital health ecosystems.	l Health
et al. (2024) [58]	ıatic review on public willingness for secondary data use; found conditional support l vacy, trust, dynamic consent, and clear benefit communication.	dary Use / Public Attitudes
n et al. (2023) [9]	of-the-art literature review on digital health consent from patient perspectives; i ences for transparency, dynamic consent, and control over PHI.	l Health
ı et al. (2023) [10]	ved public preferences for transparency in secondary data use; highlighted demand for unication, control, and ethical oversight.	dary Use of Health Data
et al. (2024) [44]	uced a blockchain-based consent model for Health Information Exchange (HIE), ensu able logging, patient control, and streamlined data access.	Information Exchange
Lee (2022) [18]	ptual framework for applying dynamic consent in pervasive healthcare, focusing on pri IoT and ubiquitous computing environments.	ive Healthcare / IoT
ızadeh (2025) [59]	ghts patient-centered integration of AI by emphasizing informed consent and p omy	al Workflows in Ophthalmology
ar et al. (2024) [60]	es patient empowerment through data ownership and control by assessing professio on patients' rights to own, control, and decide use of their genomic data, emphas ıic consent	Centric Genomic Data Managem
& In (2024) [56]	chain and smart contracts enable data self-sovereignty by giving users full ownership, co ccess, sharing, and portability of their data, supporting user-centric and censorship-res anagement.	vereign decentralized storage

Legal and Ethical Alignment

Compliance with privacy regulations such as GDPR and the EHDS was discussed in 19 out of 55 studies (35%). Most frameworks aimed to align with GDPR principles of informed and revocable consent (Article 7) and data minimisation (Article 5). A recurring challenge was the conflict between blockchain immutability and GDPR's right to erasure (Article 17). To address this, several systems employed privacy-preserving designs, recording only hashed references or using off-chain pointers to revocable consent states. Only 9 out of 55 studies (16%) addressed the "right to erasure" (Article 17) directly, highlighting the continuing tension between blockchain immutability and deletion requirements. Specifically 12 out of 55 studies (22%) used off-chain storage of personal data and on-chain hash references; 6 out of 55 studies (11%) adopted revocable credentials or tokenized pseudonyms to enable logical deletion; and 3 out of 55 studies (5%) explored ZKPs to verify consent without revealing personal data [42], although these remained largely experimental.
The works presented in [19,50] linked blockchain consent to EHDS and EUDI wallet frameworks, indicating an emerging policy-driven research direction. Nonetheless, ethical analysis remained superficial in most papers, only 8 out of 55 studies (15%) explicitly referenced bioethical principles such as autonomy, justice or beneficence.

Beyond such high-level alignment claims, concrete operational guidance for EHDS is now emerging. The TEHDAS guideline to Health Data Access Bodies provides detailed recommendations on implementing opt-out from secondary use, including the establishment of national opt-out registries, citizen-facing portals, and cross-border recognition of opt-out choices. This underscores that EHDS compliance for blockchain-based consent systems requires integration with HDAB governance and institutional workflows, not only on-chain auditability or consent logic [3].

Furthermore, [61,62] provides a comprehensive legal analysis revealing that existing EU data protection frameworks, including the GDPR and the EHDS Regulation, inadequately support the lawful and harmonized secondary use of health and genetic data across borders, and it advocates for new EU-level legislative measures to establish consistent legal bases for such data reuse. The work [36] introduces the novel concept of "demonstrated consent," a blockchain- and generative AI–based framework that uses NFTs and large language models to create a transparent, participant-centered system for managing, tracking, and communicating biobanking consent. Also, [63] provides a comprehensive analysis of the conflicts between blockchain's immutability and data protection requirements, proposing a hybrid legal-technical framework that leverages off-chain storage, encryption, and privacy-enhancing technologies to achieve regulatory compliance while preserving blockchain's core functionalities.

Thus, while legal alignment is widely acknowledged, comprehensive ethical governance and juridical interpretation of blockchain consent remain underdeveloped. Table 7 summarizes the studies that explicitly address legal and ethical alignment across these dimensions.

Table 7. Studies Addressing Legal & Ethical Alignment

Authors & Date	Legal/Ethical Focus	Application Area
i et al. (2022) [25]	ed a GDPR-compliant, decentralized consent system for wearable fitness data hain and smart contracts	ble Fitness Data / Healthcare
al. (2024) [20]	sed a GDPR-compliant hybrid architecture with a "purpose tree" for consent managem	al GDPR Consent Management (ap thcare)
al. (2025) [64]	sed a blockchain-based EMR sharing method with ring signatures and off-chain sto d security, privacy, transparency, and compliance with China's PIPL.	onic Medical Records (EMR)
et al. (2022) [53]	sed a blockchain-based privacy-preserving data governance framework ens ntability, transparency, and compliance across multiple stakeholders.	Stakeholder Data Governance (hea lomain)
dt et al. (2025) [8]	g review mapping technical implementations of informed consent in digital health; iden ges (obtain, prove, retrace, manage), highlighted blockchain and dynamic consel sing but under-evaluated.	Health / mHealth Consent
en et al. (2020) [6	zed regulatory and legal challenges of data sharing in clinical trials under GDPR; focus iance, transparency, and secondary use of data.	al Trials / Legal & GDPR Complian
al. (2024) [66]	ed best practices for data minimization, anonymization, pseudonymization, encryption on; applied case study in healthcare dataset; highlighted ethical and regulatory compli	se Management / Healthcare Datas
a et al. (2021) [67	w of GDPR impacts on biomedical research and consent; called for harmonization of lav clarification of broad consent, and roadmap for secondary data use.	dical Research Governance
et al. (2023) [14]	-based study showing patients prefer dynamic consent and continuous communicati scale data reuse; emphasized patient-centric governance.	Scale Health Data Reuse
r et al. (2020) [34	uced dynamic informed consent for large-scale genomics; highlighted ethical challeng icing and proposed dynamic consent as a solution for transparency and patient control.	ics / Population Sequencing
et al. (2025) [36]	uced "demonstrated consent": a hybrid model combining blockchain (NFTs tied to sam nerative AI (LLMs) for interactive, transparent communication in biobanking.	king
et al. (2023) [37]	sed a formal security model for DCMS; introduced definitions of confidentiality, availat eability, auditability; suggested integrating blockchain, differential privacy, and ic Consent in e-Healthcare ledge Proofs (ZKPs) to strengthen privacy-by-design.
et al. (2024) [68]	analysis of EU data protection law and ethical issues for secondary use of health/genetic current GDPR framework insufficient, recommending new legislation.	dary Use of Health & Genetic Data
et al. (2024) [58]	natic review on public willingness for secondary data use; found conditional support l vacy, trust, dynamic consent, and clear benefit communication.	dary Use / Public Attitudes
a et al. (2023) [10	ved public preferences for transparency in secondary data use; highlighted demand for unication, control, and ethical oversight.	dary Use of Health Data
et al. (2023) [42]	ed decentralized privacy-first DCMS with patient empowerment; used blockcha ralize consent and ensure transparency.	thcare
2025) [63]	technical review of conflicts between blockchain immutability and GDPR rights; sugg architectures and privacy-preserving techniques.	rotection / Legal-Tech
azadeh (2025) [59	es a comprehensive ethical and regulatory analysis of AI in ophthalmology	pthalmology
ar et al. (2024) [6	sional perspectives on patient data ownership, collective and laboratory ownership, copy ations, GDPR-like privacy concerns	overnance

Summary of Thematic Prevalence

To consolidate the thematic findings across the 55 reviewed studies, Table 8 summarizes the dominant design approaches, associated methodological characteristics, and proportional representation across the four analytical dimensions examined earlier. The purpose of this synthesis is to provide a holistic overview of how blockchain-based dynamic consent systems distribute their priorities between technical, usability, and regulatory domains, and to indicate areas where further development and evaluation are needed.

Table 8. Summary of thematic prevalence across the reviewed studies

ical Dimension	ninant Approach	Studies (n) / %
nt Lifecycle Management	contract–based grant/modify/revoke models	35 / 64 %
bility & Traceability	l on/off-chain hash-anchoring systems	27 / 49 %
ity & Empowerment	r mobile interfaces (with limited testing)	19 / 35 %
& Ethical Alignment	-compliant off-chain designs	19 / 35 %

These findings reflect a rapidly converging landscape in which blockchain technologies are increasingly adopted as trust anchors for consent tracking, audit logging, and integrity assurance. However, striking divergences remain in how thoroughly these patterns are implemented and evaluated. Most studies incorporate blockchain for immutable auditability, but fewer extend the evaluation to human-centered usability or cross-system enforcement of consent withdrawal. As detailed in the Consent Lifecycle Management analysis, revocation propagation beyond on-chain state updates remains rarely implemented and largely unvalidated in current blockchain-based consent frameworks.

To further clarify how recurring technical mechanisms align with European regulatory frameworks, Tables 9-11 disaggregate the previously consolidated analysis into goal-specific comparisons, focusing on data storage, consent and access enforcement, and auditability and interoperability, respectively. This restructuring enables direct comparison of how the same functional objectives are implemented across different blockchain-based consent frameworks and addresses the overlapping nature of design choices observed in the literature.

Table 9 compares data storage and persistence strategies adopted by the reviewed studies. A clear convergence emerges toward off-chain storage combined with on-chain hash anchoring, which enables integrity verification and auditability while supporting data minimization and erasure requirements under GDPR Articles 5 and 17. Nevertheless, a small subset of studies, primarily proof-of-concept designs propose storing encrypted health data or metadata directly on-chain. Such approaches raise significant regulatory and security concerns, particularly with respect to the right to erasure and long-term exposure risks, and remain misaligned with GDPR and EHDS expectations.

Table 10 focuses on consent and access enforcement mechanisms. Most reviewed frameworks rely on smart contracts combined with off-chain policy enforcement points (PEPs) or token-based authorization to enable revocable and fine-grained access control. While these mechanisms support logical revocation under GDPR Article 7, enforcement is often partial and dependent on timely synchronization between on-chain consent state and off-chain systems. As a result, revocation propagation delays and stale authorization caches remain recurring limitations across implementations.

Table 11 summarizes approaches to auditability and interoperability. Immutable on-chain logs are widely used to ensure non-repudiation and traceability but are rarely human-readable or directly usable by regulators or patients. Emerging approaches that bridge blockchain events with healthcare standards such as HL7 FHIR Consent and AuditEvent resources demonstrate greater potential for institutional governance and EHDS-aligned interoperability, although adoption remains limited and implementations are still evolving.

Table 9. Data storage and persistence strategies in blockchain-based consent frameworks

Strategy	On-chain data	Typical use	Regulatory alignment	Key risk
ıain + hash anchoring		ity, audit		linkage
pted on-chain storage		lesigns		re impossible

Table 10. Consent and access enforcement mechanisms for secondary use of health data

Mechanism	Revocable	Enforcement scope	Limitation
contracts + PEP	l		cy
ı-based consent			staleness

Table 11. Auditability and interoperability approaches in blockchain-enabled consent systems

Approach	Human-readable	Standards aligned	Limitation
ıain logs			ısability
AuditEvent anchoring			adoption

Taken together, this goal-based analysis reinforces that blockchain is not inherently compliant or sufficient on its own. Regulatory alignment depends on how architectural components operationalize principles such as data minimization, revocability, accountability, and interoperability. Although architectural convergence is evident across storage and audit patterns, substantial gaps remain in enforcement assurance, usability validation, and governance integration.

Quantitative summary, quality assessment and emerging trends

This section synthesizes the core quantitative findings from the 55 studies, evaluates their methodological quality, and highlights emerging architectures and research trajectories in blockchain-based dynamic consent for secondary health data use, with particular attention to how study quality influences the strength of reported design claims.

As discussed in the Consent Lifecycle Management analysis, sensitivity analysis restricted to higher-quality studies (QI ≥ 0.75) further confirms that operational revocation propagation beyond on-chain state changes remains rarely implemented and empirically unvalidated. Similarly, the proportion of studies reporting formal usability evaluation remained below 25%. Core architectural trends, such as hybrid on-chain/off-chain storage and smart contract–based consent modelling, remained consistent across quality thresholds. This indicates that while foundational design patterns are robust, claims related to operational enforceability and real-world readiness are supported by a limited subset of higher-quality studies.

Quantitative Overview

A structured synthesis of the extracted data reveals strong convergence on several foundational design patterns for blockchain-based consent management. Table 12 presents the operational definitions and associated aggregate counts derived during quantitative coding.

Table 12. Operational definitions and counts used in the quantitative synthesis

Metric	Operational definition	Count (n/N)	Percent
:hain consent system	proposes or evaluates a consent framework implemented on blockchain/DLT with execu ıt logic or on-chain logging.	43/55	78.2
ıic/ revocable consent	work allows post-hoc modification and/or withdrawal of consent enforced by smart cont chain controllers (not merely discussed conceptually).	39/55	
ıterface present	ype or product UI shown for patients/stakeholders to manage consent.	16/55	
l usability testing	ts a recognized method (e.g., SUS/UEQ/think-aloud) with N and procedure.	11/55	
bility implemented	ain or hybrid logging built, not only proposed.	18/55	

These proportions reflect a strong trend toward technical feasibility and decentralized audit trails, with less attention to user-facing evaluative studies. In particular, fewer than one in five studies (<20%) report user experience validation, despite claims of user empowerment and transparency.

Publication trends from 2020 to 2025 show an accelerating interest in the topic, with a marked surge beginning in 2022. This aligns with regulatory movement around the European Health Data Space (EHDS) and the maturation of decentralized identity standards, such as W3C DIDs and VCs.

Quality and agreement Assessment

To evaluate the reliability and robustness of the reviewed studies, a five-item Quality Index (QI) was applied across all papers, scoring on clarity of objectives, architectural transparency, consent lifecycle coverage, privacy/regulatory alignment, and empirical validation. The resulting QI scores ranged from 0.35 to 0.95, with a median of 0.68 (IQR: 0.54–0.82), indicating overall moderate to high methodological quality.

- Inter-rater agreement was substantial ($\kappa = 0.78$; range: 0.71–0.85).
- Excluding studies with QI < 0.50 slightly reduced thematic counts (e.g., dynamic consent: 39 → 33) but did not reverse key trends.
- Notably, automated revocation propagation across system boundaries remains rare and empirically unvalidated, with no studies reporting latency or enforcement assurance metrics, representing an operational gap with direct implications for GDPR compliance (Article 7).

Beyond reporting agreement, the quality assessment provides critical interpretive context for the thematic synthesis. Studies with higher QI scores consistently offered clearer architectural descriptions, explicit consent-state models, and at least partial empirical validation, whereas lower-QI studies were more likely to present conceptual frameworks without implementation detail or reproducible evaluation.

When restricting the analysis to studies with QI ≥ 0.75, several commonly reported capabilities, particularly around real-time revocation propagation and user empowerment were supported by only a very small subset of works, indicating that these features remain largely aspirational rather than operationally demonstrated in the current literature.

Similarly, claims of GDPR or EHDS compliance in lower-QI studies were often based on high-level alignment statements rather than concrete legal–technical mechanisms (e.g., explicit handling of Article 17 erasure or cross-system enforcement), whereas higher-QI studies more frequently implemented hybrid storage, revocable credentials, or auditable consent-state transitions.

Taken together, these results emphasize that while the foundational architectural patterns for blockchain-enabled dynamic consent are maturing, the empirical depth needed to substantiate performance, usability, and regulatory enforcement remains limited. Evaluation rigor, latency benchmarking, and cross-institutional enforcement assurance therefore represent critical priorities for advancing from conceptual feasibility toward operational readiness.

Overall, the QI analysis suggests that the field is characterized by strong architectural innovation but uneven methodological maturity, and that future research must prioritize reproducible implementations, measurable performance indicators, and user-centered validation to strengthen the evidence base for blockchain-based consent systems in real healthcare settings.

Emerging Research and Technical Trends

Several emergent clusters signal the evolving priorities and directions in the field:

- Self-Sovereign Consent with DIDs and VCs:

Adoption of decentralized identity credentials to enable user-controlled consent traces and cross-domain portability, especially in cross-border care scenarios [50].

This trend reflects a shift from institution-centric consent registries toward patient-held, cryptographically verifiable consent artefacts, aligning with emerging EUDI Wallet and W3C VC ecosystems. However, only a limited subset of studies demonstrated live wallet integration or interoperability across domains, indicating that most implementations remain at prototype or conceptual stages.

- FHIR and HL7-aligned Interoperability:

Increasing emphasis on bridging blockchain with clinical standards (e.g., FHIR Consent and AuditEvent), in preparation for EHDS and HealthData@EU infrastructures [69].

Recent works explicitly map smart-contract consent states to FHIR Consent resources and expose blockchain audit events as FHIR AuditEvent records, signaling a growing recognition that blockchain layers must integrate with existing health IT workflows rather than operate as parallel infrastructures. Nonetheless, most proposals stop short of demonstrating production-grade interoperability or conformance testing against national FHIR profiles.

- Privacy-Preserving Cryptography:

Experimental use of zero-knowledge proofs and selective disclosure schemes for authorization without identifier exposure, aligned with GDPR Article 25.

These approaches aim to reconcile blockchain transparency with data minimization by enabling verification of consent or access rights without revealing identities or attributes. However, implementations remain limited to proof-of-concept circuits, with unresolved challenges around computational overhead, verifier scalability, and standardization across platforms.

- Hybrid Blockchain Architectures:

Use of off-chain storage with on-chain hashes or audit indices to balance GDPR erasure rights with audit integrity has been a dominant architectural pattern since early blockchain-based health data exchange systems. Rather than an emerging trend, recent studies refine this baseline by introducing richer metadata anchoring, revocable pointers, and tighter coupling with off-chain policy enforcement points, reflecting a shift from architectural choice toward operational optimization.

- Policy-Driven Design:

Many systems explicitly frame their architecture in terms of GDPR and EHDS compliance, emphasizing revocability, auditability, and patient agency.

This has led to architectures that embed legal concepts such as purpose limitation, consent expiry, and accountability directly into smart-contract logic. Nevertheless, legal alignment is often asserted rather than empirically validated, and few studies evaluate whether implemented mechanisms would satisfy regulatory scrutiny in real enforcement scenarios.

Across these trends, a common pattern emerges architectural sophistication is increasing, but empirical validation and cross-system interoperability lag behind. Higher-quality studies (QI $\geq$ 0.75) are more likely to integrate multiple trends simultaneously such as DIDs with FHIR bridging and hybrid storage suggesting that technical convergence is occurring primarily in the most methodologically mature works. Together, these trends indicate a gradual transition from conceptual feasibility toward policy-aware and interoperability-oriented design. However, significant gaps persist in enforcement interoperability, large-scale deployment evidence, usability testing, and latency assurance, underscoring that most frameworks remain pre-operational despite increasing architectural convergence.

Discussion

Summary of Main Findings

This systematic review analyzed 55 peer-reviewed studies published between 2020 and 2025 that proposed or evaluated blockchain-based frameworks for dynamic and revocable consent in the secondary use of health data. The findings indicate that most proposed systems leverage smart contracts and hybrid on-chain/off-chain architectures to support consent lifecycle management and immutable auditability. While dynamic consent and revocation are frequently claimed features, only a small subset of studies provided architectural detail or empirical evidence demonstrating automated revocation propagation across distributed systems. Usability evaluation and real-world deployment remain limited, with fewer than one-fifth of studies reporting formal user testing. Furthermore, although GDPR alignment is commonly asserted, explicit consideration of the European Health Data Space (EHDS) governance model and operational opt-out mechanisms is still sparse.

Sensitivity analysis based on methodological quality (QI $\geq$ 0.75) confirmed that high-level architectural patterns remain stable, whereas evidence for automated revocation propagation, usability validation, and enforcement assurance is limited to a small subset of higher-quality studies.

Dynamic and Revocable Consent Lifecycle Management

In relation to the first objective of this review, characterizing architectural and operational approaches to dynamic and revocable consent blockchain was widely adopted as an enabling infrastructure for managing dynamic and revocable consent lifecycles in healthcare. Most frameworks employed smart contracts to automate consent processes, recording events such as consent granting, modification, and revocation, and defining granular access conditions including time-bound or purpose-specific authorizations. By encoding consent states on-chain, these systems leveraged blockchain's immutability to maintain verifiable histories of consent actions, conceptually aligning with principles of patient autonomy and ongoing informational self-determination.

However, despite frequent claims of revocability, the practical realization of dynamic consent remained limited. Only a small fraction of studies operationalized real-time revocation propagation across distributed data custodians, and many implementations relied on simulated environments rather than live data-sharing scenarios. Even among higher-quality studies, revocation was typically enforced through local policy decision points querying on-chain consent state, rather than through end-to-end automated propagation across institutional boundaries. As a result, most frameworks achieved logical revocability at the ledger level but did not demonstrate effective enforcement across heterogeneous, off-chain data environments.

The increasing integration of decentralized identifiers (DIDs) and verifiable credentials (VCs) reflects a broader shift toward self-sovereign consent models, enabling individuals to assert and manage permissions independently of central authorities. Nevertheless, most DID- and VC-enabled systems stopped short of demonstrating cross-domain portability or wallet-to-wallet interoperability, indicating that self-sovereign consent remains largely aspirational. From a regulatory perspective, this gap is significant, as both the GDPR and the EHDS require not only the possibility of consent withdrawal but its practical and timely effect on ongoing and future data processing.

The limited operationalization of revocation propagation observed in this review reflects a combination of technical, regulatory, and organizational factors rather than a lack of conceptual awareness. From a technical perspective, propagating consent withdrawal across distributed data custodians requires reliable event dissemination, low-latency synchronization, and tight coupling between blockchain layers and off-chain access control systems, capabilities that are difficult to implement and evaluate in academic prototypes. From a regulatory standpoint, uncertainty persists regarding how blockchain-based "logical deletion" mechanisms are interpreted under GDPR Article 17 and how these mechanisms will align with the EHDS governance model, particularly in federated infrastructures such as HealthData@EU. Organizationally, many proposed systems lack clear institutional incentives or compliance drivers to validate revocation enforcement beyond the ledger level, resulting in designs that prioritize auditability over enforceability. Together, these factors help explain why revocation is widely claimed but rarely demonstrated as an end-to-end operational capability.

Auditability, Provenance, and Accountability

Addressing the second objective of assessing auditability and accountability mechanisms, auditability and provenance tracking emerged as among the most consistently addressed features of blockchain-based consent frameworks. Many studies capitalized on blockchain's tamper-evident recordkeeping to provide verifiable logs of consent events and data access transactions, underpinning accountability in multi-institutional and cross-border data reuse scenarios. Three dominant design patterns were observed: direct on-chain audit logging, hybrid architectures anchoring off-chain logs on-chain, and smart-contract state verification through read-only queries.

Hybrid audit models were the most prevalent, reflecting a balance between transparency, privacy, and scalability. These approaches typically stored detailed audit metadata off-chain while anchoring cryptographic proofs on-chain, allowing integrity and non-repudiation without exposing sensitive identifiers. Such configurations are particularly relevant in GDPR and EHDS contexts, where data minimization and controlled disclosure are essential. Architecturally, this trend also coincides with a move away from public, permissionless blockchains toward permissioned or consortium-based ledgers governed by trusted healthcare or research institutions.

Despite strong technical guarantees, auditability often did not translate into practical accountability. Only a limited number of studies provided user-facing audit dashboards or regulator-oriented reporting tools, leaving audit data opaque to non-technical stakeholders. In many cases, audit logs were verifiable by machines but inaccessible or unintelligible to patients, ethics committees, or oversight authorities. This highlights that accountability is not solely a cryptographic property but a socio-technical one, requiring human-readable representations and institutional governance interfaces.

Emerging efforts to integrate blockchain logs with established healthcare standards, such as HL7 FHIR AuditEvent resources, represent a promising direction. However, these remain early-stage, and standardized frameworks for consent provenance visualization and regulatory reporting are still under development.

Usability, Interoperability, and Operational Constraints

With respect to the objective of evaluating usability, interoperability, and implementation maturity, usability and real-world adoption remain persistent challenges. Only a minority of studies reported formal usability testing or user experience evaluation, and many systems required interactions with cryptographic wallets, private keys, or blockchain transactions that

exceed typical patient or clinician digital literacy. These challenges assumptions underlying self-sovereign models and underscores the need for human-centered design approaches.

Frameworks incorporating mobile-friendly consent dashboards or DID wallets demonstrated greater potential for user acceptance, yet accessibility barriers such as limited multilingual support, unclear consent visualization, and insufficient mobile optimization were common. Studies with higher methodological quality were more likely to report participatory design or usability validation, reinforcing the link between technical maturity and user-centered evaluation.

Interoperability with existing health information systems also emerged as a critical bottleneck. Although several studies referenced integration with electronic health records or HL7 FHIR resources, few described concrete mechanisms for synchronizing blockchain-based consent states with institutional access control systems or cross-border infrastructures. Without standardized interfaces and data models, blockchain-based consent solutions risk operating in isolation from clinical and research workflows, limiting their production viability. Increasingly, blockchain appears best positioned as a coordination and trust layer rather than a replacement for established health IT systems.

Scalability and performance concerns further constrain deployment. Most frameworks adopted permissioned ledgers or layer-2 solutions to address throughput and cost limitations, yet latency in consent updates and revocation propagation remains largely unmeasured. The near absence of reported performance benchmarks suggests that scalability is often assumed rather than empirically validated.

Regulatory Alignment and Ethical Governance

Most reviewed studies explicitly referenced compliance with the GDPR, particularly requirements for informed and revocable consent. However, alignment was more often asserted than operationalized. The tension between blockchain immutability and rights such as erasure remains unresolved in many designs, with mitigation strategies such as off-chain storage, revocable credentials, or zero-knowledge proofs still largely experimental.

With the EHDS Regulation establishing dedicated governance structures for secondary use of health data in the European Union, future consent architectures must increasingly move beyond GDPR-centric interpretations. Compliance under the EHDS depends not only on technical design but also on integration with HealthData@EU infrastructures, certification schemes, and institutional access bodies. Ethical governance was comparatively underdeveloped across the literature, with limited engagement with principles such as justice, beneficence, or the ethical implications of automated consent enforcement.

Comparison with Existing Reviews

Several prior reviews have examined blockchain applications in healthcare or digital consent from complementary perspectives; however, their analytical scope differs substantially from that of this review. Surveys focusing on blockchain in healthcare have primarily emphasized data security, interoperability, or application domains such as clinical trials and supply chains, without systematically analyzing consent as a dynamic and revocable lifecycle with enforceable propagation mechanisms. Conversely, reviews of digital or dynamic consent have largely centered on ethical, legal, or usability considerations, often without examining the underlying technical architectures required to ensure verifiable auditability and distributed enforcement.

In contrast to these earlier works, this review explicitly integrates architectural, operational, and regulatory dimensions by examining how blockchain-based frameworks implement consent lifecycle management, auditability, usability, and legal alignment for secondary use of health data. By synthesizing evidence from 55 peer-reviewed studies published between 2020 and 2025, this review advances prior literature in three key ways. First, it systematically analyses revocation enforcement and propagation mechanisms, revealing that revocability is frequently asserted but rarely operationalized across distributed data custodians. Second, it evaluates auditability not only as a cryptographic property but also as a socio-technical capability requiring interpretability and governance integration. Third, it situates blockchain-based consent frameworks within the emerging European Health Data Space (EHDS) regulatory context, which has been largely absent from previous reviews.

By consolidating fragmented evidence across technical, usability, and regulatory dimensions, this review moves beyond descriptive surveys and provides an integrative assessment of the operational maturity of blockchain-enabled consent systems. This positioning clarifies both the current limitations of existing approaches and the concrete design and governance challenges that must be addressed to enable real-world deployment for secondary use of health data.

Positioning this review within the broader consent literature reveals a clear progression in research focus. Reviews of dynamic consent outside blockchain contexts have predominantly examined ethical acceptability, user engagement, and governance models, often assuming centralized infrastructures and institutional enforcement. Conversely, surveys of blockchain in healthcare have focused on data security, provenance, and interoperability, treating consent as a secondary or implicit function rather than as a programmable lifecycle.

This review differs by explicitly integrating these trajectories. By analyzing consent as an enforceable lifecycle implemented through blockchain-based architectures, the review links ethical expectations of dynamic consent with the technical mechanisms required to operationalize revocation, auditability, and accountability in distributed secondary-use settings. In doing so, it exposes a persistent gap between conceptual consent models and their technical realization, particularly in

relation to revocation propagation and cross-institutional enforcement an aspect not systematically examined in earlier reviews.

Implications for Design, Governance, and Policy

The findings suggest that future progress depends less on novel blockchain primitives and more on integrative system design. Blockchain should be treated primarily as a coordination and accountability layer rather than as a data repository. Effective systems must tightly couple on-chain consent states with off-chain policy enforcement points, adopt interoperable standards such as HL7 FHIR for consent and audit representation, and embed legal interpretation into system governance.

From an institutional perspective, consortium-based deployments with clear roles and accountability mechanisms are better aligned with secondary-use contexts than public infrastructures. For policymakers and standards bodies, clearer guidance is needed on how blockchain-enabled consent can interoperate with EHDS governance models, including HealthData@EU and Health Data Access Bodies.

The observed variation across application domains, blockchain platforms, and system maturity suggests that blockchain-enabled consent solutions are not uniform and should not be evaluated as a single class of systems. Design trade-offs that are acceptable in clinical trial environments, such as controlled participation and sponsor oversight, may not translate directly to large-scale EHR or population-health infrastructures. Similarly, while public blockchains support rapid prototyping and transparency, permissioned and consortium deployments appear more compatible with regulated secondary-use contexts under GDPR and the EHDS. These differences underscore the need for domain-sensitive evaluation rather than one-size-fits-all architectural assumptions.

Toward an Operational Research Agenda for Blockchain-Based Dynamic Consent

To move beyond high-level design principles, the findings of this review motivate a concrete research agenda focused on operational validation rather than architectural novelty. First, future work should prioritize the design and evaluation of a multi-site revocation propagation protocol, in which consent withdrawal events recorded on-chain are automatically disseminated to heterogeneous off-chain policy enforcement points operated by independent institutions. Such a protocol should explicitly define event subscription mechanisms, enforcement acknowledgment semantics, and failure-handling procedures, enabling revocation to be evaluated as a measurable system property rather than a conceptual claim.

Second, pilot studies should report quantitative enforcement metrics, including revocation propagation latency, completeness of enforcement across data custodians, and system behavior under partial network or service failures. These metrics are directly relevant to GDPR Article 7 and EHDS requirements that withdrawal of consent have timely and practical effect, yet they are absent from current implementations.

Third, human-centered design should be operationalized through participatory pilot deployments rather than interface descriptions alone. For example, wallet-based consent systems could be evaluated through longitudinal studies assessing user comprehension of consent states, revocation confidence, and perceived control when consent decisions have observable downstream effects.

Finally, interoperability claims should be validated through standards-based integration pilots, mapping smart-contract consent states to HL7 FHIR Consent and AuditEvent resources and testing end-to-end workflows within EHDS-aligned infrastructures such as HealthData@EU. Together, these directions define a transition from conceptual feasibility toward deployment-ready, regulatorily meaningful consent infrastructures.

Future Research Directions

Future research should prioritize end-to-end revocation enforcement as a measurable system property, rather than treating revocation solely as an on-chain state transition. This includes the explicit design and evaluation of revocation propagation protocols that disseminate withdrawal events from blockchain ledgers to heterogeneous off-chain policy enforcement points operated by independent data custodians. Such protocols should be evaluated using quantitative metrics, including propagation latency, enforcement completeness, and system behavior under partial failures.

In parallel, interoperability with EHDS-aligned infrastructures should move beyond architectural claims toward standards-based validation. Future studies should assess how blockchain-based consent states and audit events can be mapped to HL7 FHIR Consent and AuditEvent resources and exercised within cross-institutional workflows anticipated by HealthData@EU. These evaluations are essential to demonstrate regulatory readiness under the EHDS governance model.

Usability and patient empowerment should likewise be examined through longitudinal, user-centered evaluations rather than interface descriptions alone. In particular, future work should assess whether patients can meaningfully understand, manage, and trust consent withdrawal when revocation has observable downstream effects on data access. Wallet-based and credential-based consent models warrant participatory studies that measure comprehension, confidence, and perceived control over time.

Finally, advancing blockchain-enabled consent from prototype to practice will require interdisciplinary pilot deployments involving technologists, clinicians, legal scholars, ethicists, and policymakers. Such collaborations are necessary to align technical enforcement mechanisms with legal interpretation, institutional governance, and real-world operational constraints.

Conclusion

This systematic review examined 55 peer-reviewed studies (2020–2025) that propose or evaluate blockchain-enabled approaches to dynamic, auditable, and revocable consent for the secondary use of health data. The synthesis demonstrates clear architectural convergence: most systems rely on hybrid on-chain/off-chain designs, use smart contracts or equivalent logic to represent consent states, and employ blockchain primarily as an integrity, coordination, and audit layer rather than as a storage substrate for sensitive health information. Many frameworks further integrate DIDs and VCs to bind consent states to portable identities and attributes, reinforcing the shift toward self-sovereign yet auditable consent artefacts.

Beyond documenting these trends, this review contributes novel insight by systematically evaluating consent as an enforceable lifecycle rather than as a static design feature, linking architectural choices to revocation propagation, usability evidence, and regulatory readiness for secondary-use governance under the GDPR and the European Health Data Space (EHDS).

The evidence indicates that blockchain can substantively strengthen two aspects of secondary-use governance. First, it provides a shared, tamper-evident ledger for recording consent decisions and access events, improving verifiability and accountability across organizational boundaries. Second, it enables programmable consent modelling, granular permissions, time-bound authorizations, and policy-driven transitions supporting the core intent of dynamic consent.

However, the review identifies a decisive gap between architectural feasibility and operational readiness. While revocation is widely claimed, most implementations demonstrate revocation only as an on-chain state transition or token invalidation, without validated propagation and enforcement across distributed off-chain systems. Sensitivity analysis restricted to higher-quality studies (QI $\geq$ 0.75) confirms that operational revocation enforcement is demonstrated by only a small subset of works, with none reporting quantitative guarantees for revocation latency or completeness across data custodians. From a regulatory standpoint, this is material: both GDPR and the EHDS framework require withdrawal to have practical and timely effect, not merely representational status, particularly in federated secondary-use infrastructures such as HealthData@EU.

A further cross-cutting finding is that technical auditability does not automatically translate into practical accountability. Many systems provide cryptographic proofs and transaction logs that are difficult for patients, auditors, and regulators to interpret. Moreover, despite frequent claims of patient empowerment, formal usability validation remains limited, and the cognitive burden associated with wallets, signing flows, and key custody continues to pose a barrier to real-world deployment.

Overall, this review demonstrates that while blockchain is a promising trust anchor for consent lifecycle tracking and auditability in secondary use of health data, it is not inherently compliant or sufficient on its own. Regulatory alignment depends on the broader socio-technical system, including enforcement mechanisms, interoperability with health IT infrastructures, governance arrangements, and user experience. Achieving operational maturity will therefore require governance-oriented design, quantitative evaluation of enforcement properties, and close integration with emerging European health data infrastructures.

This review advances the consent literature by reframing blockchain-based consent from a static compliance artifact to an enforceable, distributed lifecycle subject to measurable system properties such as revocation latency, propagation completeness, and governance integration. Unlike prior surveys, it systematically links architectural design choices to operational enforceability and emerging EHDS governance requirements, revealing that most existing systems remain at a proof-of-concept stage with limited real-world assurance.

Funding

This work did not receive any external funding.

Data Availability

The datasets analyzed during this study are available from the corresponding author upon reasonable request

Authors' Contributions

JCF conceptualized the work, SP and MB conducted data extraction, formal analysis, synthesis and initial draft preparation, RB and JCF supervised and revised the original draft, JCF funding acquisition and resources

Conflicts of Interest

The authors declare that they have no known financial, commercial, or personal conflicts of interest that could have appeared to influence the work reported in this manuscript. The research was conducted independently, and no external entity had any role in the study design, data collection, analysis, interpretation of results, or the decision to submit the article for publication.

Multimedia Appendix 1

PRISMA based literature analysis and the summary of findings of the selected articles, their categorical classification are presented.

References

1. Phuyal S, Elvas LB, Ferreira JC, Bista R. Blockchain Technology in Healthcare: Unifying Patient Medical Records - A Survey. In: Sakalauskas V, Bajaj A, Abraham A, Madhavi KR, Manghirmalani Mishra P, editors. Bio-Inspired Comput Cham: Springer Nature Switzerland; 2025. p. 319–332. doi: 10.1007/978-3-031-78946-5_31ISBN:978-3-031-78945-8
2. Global strategy on digital health 2020-2025. 2021. Available from: https://www.who.int/publications/i/item/9789240020924 [accessed Oct 28, 2025]
3. Draft guideline to Health Data Access Bodies: How to implement opt-out from secondary use of electronic health data. TEHDAS2 Joint Action; 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 [accessed Dec 25, 2025]
4. 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). Feb 11, 2025. Available from: http://data.europa.eu/eli/reg/2025/327/oj/eng [accessed Aug 14, 2025]
5. Albalwy F, Brass A, Davies A. A Blockchain-based dynamic consent architecture to support clinical genomic data sharing (ConsentChain): Proof-of-concept study. JMIR Med Inform. JMIR Publications Inc.; 2021. doi: 10.2196/27816
6. Hang L, Chen C, Zhang L, Yang J. Blockchain for applications of clinical trials: Taxonomy, challenges, and future directions. IET Commun. John Wiley and Sons Inc; 2022. p. 2371–2393. doi: 10.1049/cmu2.12488
7. Baysal MV, Özcan-Top Ö, Betin-Can A. Blockchain technology applications in the health domain: a multivocal literature review. J Supercomput. Springer; 2023. p. 3112–3156. doi: 10.1007/s11227-022-04772-1
8. Schmidt R, Schiering I, Zwingelberg H, Friedewald M. Challenges and Solutions in Implementing Informed Consent in Digital Environments: A Scoping Review. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2025. p. 71965–71983. doi: 10.1109/ACCESS.2025.3562773
9. Kassam I, Ilkina D, Kemp J, Roble H, Carter-Langford A, Shen N. Patient Perspectives and Preferences for Consent in the Digital Health Context: State-of-the-art Literature Review. J Med Internet Res. JMIR Publications Inc.; 2023. PMID:36763409
10. Cumyn A, Ménard J-F, Barton A, Dault R, Lévesque F, Ethier J-F. Patients' and Members of the Public's Wishes Regarding Transparency in the Context of Secondary Use of Health Data: Scoping Review. J Med Internet Res. JMIR Publications Inc.; 2023. PMID:37052967
11. Dave P. How Digital Health is Revolutionizing Healthcare and Contributing to Positive Health Outcomes. J Drug Deliv Ther 2024 June 15;14(6):287–293. doi: 10.22270/jddt.v14i6.6640
12. Thomason J. Big tech, big data and the new world of digital health. Glob Health J 2021 Dec;5(4):165–168. doi: 10.1016/j.glohj.2021.11.003
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). OJ L Apr 27, 2016. Available from: http://data.europa.eu/eli/reg/2016/679/oj [accessed Nov 3, 2025]
14. Muller SH, van Thiel GJ, Mostert M, van Delden JJ. Dynamic consent, communication and return of results in large-scale health data reuse: Survey of public preferences. Digit Health. SAGE Publications Inc.; 2023. doi: 10.1177/20552076231190997
15. Albanese G, Calbimonte J-P, Schumacher M, Calvaresi D. Dynamic consent management for clinical trials via private blockchain technology. J Ambient Intell Humaniz Comput. Springer Science and Business Media Deutschland GmbH; 2020. p. 4909–4926. doi: 10.1007/s12652-020-01761-1
16. Noë A, Vaillancourt E, Zawati MH. Verbal consent in biomedical research: moving toward a future standard practice? Front Genet Frontiers; 2025 Feb 28;16. doi: 10.3389/fgene.2025.1472655
17. Yang X, Tong B. Efficient and revocable privacy-preserving medical data sharing scheme with data integrity. J Supercomput 2025 Apr 16;81(6):751. doi: 10.1007/s11227-025-07238-2
18. Lee H, Lee U. Toward Dynamic Consent for Privacy-Aware Pervasive Health and Well-being: A Scoping Review and Research Directions. IEEE Pervasive Comput 2022 Oct;21(4):25–32. doi: 10.1109/MPRV.2022.3210747
19. Charles WM, van der Waal MB, Flach J, Bisschop A, van der Waal RX, Es-Sbai H, McLeod CJ. Blockchain-Based Dynamic Consent and its Applications for Patient-Centric Research and Health Information Sharing: Protocol for an Integrative Review. JMIR Res Protoc. JMIR Publications Inc.; 2024. doi: 10.2196/50339
20. Can O, Dag T, Kantarcioglu M. A Blockchain-Based Hybrid Architecture for Auditable Consent Management. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2024. p. 100419–100445. doi: 10.1109/ACCESS.2024.3431292
21. Anasuri S, Rusum GP. Blockchain-based identity management in decentralized applications. Int J AI BigData Comput Manag Stud 2022;3(3):70–81.
22. Hovorushchenko T, Moskalenko A, Osyadlyi V. Methods of medical data management based on blockchain technologies. J Reliab Intell Environ. Springer Science and Business Media Deutschland GmbH; 2023. p. 5–16. doi: 10.1007/s40860-022-00178-1

23. Zotero | Your personal research assistant. Available from: https://www.zotero.org/ [accessed Feb 8, 2026]
24. Kim JW, Kim SJ, Cha WC, Kim T. A Blockchain-Applied Personal Health Record Application: Development and User Experience. Appl Sci Switz. MDPI; 2022. doi: 10.3390/app12041847
25. Alhajri M, Rudolph C, Shahraki AS. A Blockchain-Based Consent Mechanism for Access to Fitness Data in the Healthcare Context. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2022. p. 22960–22979. doi: 10.1109/ACCESS.2022.3154106
26. Dong Y, Mun SK, Wang Y. A blockchain-enabled sharing platform for personal health records. Heliyon. Elsevier Ltd; 2023. doi: 10.1016/j.heliyon.2023.e18061
27. Jaiman V, Urovi V. A Consent Model for Blockchain-Based Health Data Sharing Platforms. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2020. p. 143734–143745. doi: 10.1109/ACCESS.2020.3014565
28. Peyrone N, Wichadakul D. A formal model for blockchain-based consent management in data sharing. J Log Algebr Methods Program. Elsevier Inc.; 2023. doi: 10.1016/j.jlamp.2023.100886
29. Daudén-Esmel C, Castellà-Roca J, Viejo A. Blockchain-based access control system for efficient and GDPR-compliant personal data management. Comput Commun. Elsevier B.V.; 2024. p. 67–87. doi: 10.1016/j.comcom.2023.11.017
30. Roman-Martinez I, Calvillo-Arbizu J, Mayor-Gallego VJ, Madinabeitia-Luque G, Estepa-Alonso AJ, Estepa-Alonso RM. Blockchain-Based Service-Oriented Architecture for Consent Management, Access Control, and Auditing. IEEE Access. Institute of Electrical and Electronics Engineers Inc.; 2023. p. 12726–12740. doi: 10.1109/ACCESS.2023.3242605
31. Kim H, Lee S, Kwon H, Kim E. Design and Implementation of a Personal Health Record Platform Based on Patient-consent Blockchain Technology. KSII Trans Internet Inf Syst. Korean Society for Internet Information; 2021. p. 4400–4419. doi: 10.3837/TIIS.2021.12.008
32. Mishra DK, Mehra PS. DiabeticChain: a novel blockchain approach for patient-centric diabetic data management. J Supercomput. Springer; 2025. doi: 10.1007/s11227-024-06589-6
33. Pham A, Edelson M, Nouri A, Kuo T-T. Distributed management of patient data-sharing informed consents for clinical research. Comput Biol Med. Elsevier Ltd; 2024. PMID:39121682
34. Dankar FK, Gergely M, Malin B, Badji R, Dankar SK, Shuaib K. Dynamic-informed consent: A potential solution for ethical dilemmas in population sequencing initiatives. Comput Struct Biotechnol J. Elsevier B.V.; 2020. p. 913–921. doi: 10.1016/j.csbj.2020.03.027
35. Kim TM, Lee S-J, Chang D-J, Koo J, Kim T, Yoon K-H, Choi I-Y. Dynamichain: Development of medical blockchain ecosystem based on dynamic consent system. Appl Sci Switz. MDPI AG; 2021. p. 1–20. doi: 10.3390/app11041612
36. Barnes C, Aboy MR, Minssen T, Allen JW, Earp BD, Savulescu J, Mann SP. Enabling Demonstrated Consent for Biobanking with Blockchain and Generative AI. Am J Bioeth. Taylor and Francis Ltd.; 2025. p. 96–111. doi: 10.1080/15265161.2024.2416117
37. Khalid MI, Ahmed M, Kim J. Enhancing Data Protection in Dynamic Consent Management Systems: Formalizing Privacy and Security Definitions with Differential Privacy, Decentralization, and Zero-Knowledge Proofs. Sensors. Multidisciplinary Digital Publishing Institute (MDPI); 2023. PMID:37688060
38. Huh KY, Moon SJ, Jeong S, Kim M-J, Yang W, Jeong M, Kim M-G, Lee S. Evaluation of a blockchain-based dynamic consent platform (METORY) in a decentralized and multicenter clinical trial using virtual drugs. Clin Transl Sci. John Wiley and Sons Inc; 2022. p. 1257–1268. PMID:35157788
39. Despotou G, Evans J, Nash W, Eavis A, Robbins T, Arvanitis TN. Evaluation of patient perception towards dynamic health data sharing using blockchain based digital consent with the Dovetail digital consent application: A cross sectional exploratory study. Digit Health. SAGE Publications Inc.; 2020. doi: 10.1177/2055207620924949
40. Lee AR, Koo D, Kim IK, Lee E, Kim HH, Yoo S, Kim J-H, Choi EK, Lee H-Y. Identifying facilitators of and barriers to the adoption of dynamic consent in digital health ecosystems: a scoping review. BMC Med Ethics. BioMed Central Ltd; 2023. PMID:38041034
41. Tith D, Lee J-S, Suzuki H, Wijesundara WMAB, Taira N, Obi T, Ohyama N. Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. Healthc Inform Res. Korean Society of Medical Informatics; 2020. p. 265–273. doi: 10.4258/hir.2020.26.4.265
42. Khalid MI, Ahmed M, Helfert M, Kim J. Privacy-First Paradigm for Dynamic Consent Management Systems: Empowering Data Subjects through Decentralized Data Controllers and Privacy-Preserving Techniques. Electron Switz. Multidisciplinary Digital Publishing Institute (MDPI); 2023. doi: 10.3390/electronics12244973
43. Singh A, Rathee G. Smart contract empowered dynamic consent: decentralized storage and access control for healthcare applications. Peer--Peer Netw Appl. Springer; 2025. p. 1–16. doi: 10.1007/s12083-024-01827-3
44. Rohini KR, Rajakumar PS, Geetha S. Smart Patient Consent Management Model for Health Information Exchange Based on Blockchain Technology. J Comput Sci. Science Publications; 2024. p. 730–741. doi: 10.3844/jcssp.2024.730.741
45. Castro C, Leiva V, Garrido D, Huerta M, Minatogawa V. Blockchain in clinical trials: Bibliometric and network studies of applications, challenges, and future prospects based on data analytics. Comput Methods Programs Biomed. Elsevier Ireland Ltd; 2024. PMID:39053350
46. Gondode P, Dass C, Kumar S, Malviya A, Ashwin M, Khanna P. Blockchain in Critical Care. Indian J Crit Care Med. Jaypee Brothers Medical Publishers (P) Ltd; 2025. p. 525–530. doi: 10.5005/jp-journals-10071-24991

47. Gupta R, Meena A, Dhir S. Blockchain in the age of industrial revolution: A systematic literature review using bibliometric analysis. Glob Bus Organ Excell. John Wiley and Sons Inc; 2024. p. 5–23. doi: 10.1002/joe.22242
48. Kasyapa MSB, Vanmathi C. Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies. Front Digit Health. Frontiers Media SA; 2024. doi: 10.3389/fdgth.2024.1359858
49. Nguyen T-T-A, Hsieh Y-H, Tseng C-H, Lin Y-C, Yuan S-M. Blockchain-Enabled Privacy-Preserving Ecosystem for DNA Sequence Sharing. Appl Sci Switz. Multidisciplinary Digital Publishing Institute (MDPI); 2025. doi: 10.3390/app15063193
50. Righi R da R, Rodrigues VF, da Costa CA, Eskofier B. Breaking Down the Data Path in Digital Health: From Edge to Fog and Beyond. IEEE Pervasive Comput. Institute of Electrical and Electronics Engineers Inc.; 2025. p. 70–81. doi: 10.1109/MPRV.2024.3521307
51. Felemban S, Yiu TW, Harvey M, Lim H, Zhu J, Bolton D, Ischia J. Current application of blockchain technology in healthcare and its potential roles in Urology. BJU Int. John Wiley and Sons Inc; 2025. doi: 10.1111/bju.16757
52. Huh KY, Jeong S-U, Moon SJ, Kim M-J, Yang W, Jeong M, Song I, Kwak Y-G, Lee S, Kim M-G. METORY: Development of a Demand-Driven Blockchain-Based Dynamic Consent Platform Tailored for Clinical Trials. Front Med. Frontiers Media S.A.; 2022. doi: 10.3389/fmed.2022.837197
53. Garcia RD, Ramachandran GS, Jurdak R, Ueyama J. Blockchain-Aided and Privacy-Preserving Data Governance in Multi-Stakeholder Applications. IEEE Trans Netw Serv Manag. Institute of Electrical and Electronics Engineers Inc.; 2022. p. 3781–3793. doi: 10.1109/TNSM.2022.3225254
54. Ali A, Ali H, Saeed A, Ahmed Khan A, Tin TT, Assam M, Ghadi YY, Mohamed HG. Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. Sensors. Multidisciplinary Digital Publishing Institute (MDPI); 2023. PMID:37765797
55. Goint M, Bertelle C, Duvallet C. Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems. Mathematics. MDPI; 2023. doi: 10.3390/math11071592
56. Merlec MM, In HP. Blockchain-Based Decentralized Storage Systems for Sustainable Data Self-Sovereignty: A Comparative Study. Sustain Switz. Multidisciplinary Digital Publishing Institute (MDPI); 2024. doi: 10.3390/su16177671
57. Dewan A, Eifler M, Hood A, Sanchez W, Gross M. Building a Decentralized Biobanking App for Research Transparency and Patient Engagement: Participatory Design Study. JMIR Hum Factors. JMIR Publications Inc.; 2025. doi: 10.2196/59485
58. Baines R, Stevens S, Austin D, Anil K, Bradwell H, Cooper L, Maramba ID, Chatterjee A, Leigh S. Patient and Public Willingness to Share Personal Health Data for Third-Party or Secondary Uses: Systematic Review. J Med Internet Res. JMIR Publications Inc.; 2024. PMID:38441944
59. Kazemzadeh K. Artificial intelligence in ophthalmology: opportunities, challenges, and ethical considerations. Med Hypothesis Discov Innov Ophthalmol. International Virtual Ophthalmic Research Center; 2025. p. 255–272. doi: 10.51329/mehdiophthal1517
60. Malakar Y, Lacey J, Twine NA, McCrea R, Bauer DC. Balancing the safeguarding of privacy and data sharing: perceptions of genomic professionals on patient genomic data ownership in Australia. Eur J Hum Genet. Springer Nature; 2024. p. 506–512. PMID:36631540
61. van Drumpt S, Chawla K, Barbereau T, Spagnuelo D, van de Burgwal L. Secondary use under the European Health Data Space: setting the scene and towards a research agenda on privacy-enhancing technologies. Front Digit Health Frontiers; 2025 June 19;7. doi: 10.3389/fdgth.2025.1602101
62. Forster RB, Alvarez EG, Zucco AG, Bernal-Delgado E, Diallo G, Estupiñán-Romero F, Ganna A, Gorman-Asal M, Hilmarsen C, Holub P, Hoeyer K, Rawat A, Rod NH, Vuorinen A-L, Varga TV. User journeys in cross-European secondary use of health data: insights ahead of the European Health Data Space. Eur J Public Health 2025 Sept 1;35(Supplement_3):iii18–iii24. doi: 10.1093/eurpub/ckaf096
63. Zafar A. Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways. J Cybersecurity. Oxford University Press; 2025. doi: 10.1093/cybsec/tyaf002
64. Qu X, Yang Z, Chen Z, Sun G. A consent-aware electronic medical records sharing method based on blockchain. Comput Stand Interfaces. Elsevier B.V.; 2025. doi: 10.1016/j.csi.2024.103902
65. Minssen T, Rajam N, Bogers M. Clinical trial data transparency and GDPR compliance: Implications for data sharing and open innovation. Sci Public Policy. Oxford University Press; 2020. p. 616–626. doi: 10.1093/scipol/scaa014
66. Pina E, Ramos J, Jorge H, Váz P, Silva J, Wanzeller C, Abbasi M, Martins P. Data Privacy and Ethical Considerations in Database Management. J Cybersecurity Priv. Multidisciplinary Digital Publishing Institute (MDPI); 2024. p. 494–517. doi: 10.3390/jcp4030024
67. Vlahou A, Hallinan D, Apweiler R, Argiles A, Beige J, Benigni A, Bischoff R, Black PC, Boehm F, Céraline J, Chrousos GP, Delles C, Evenepoel P, Fridolin I, Glorieux G, Van Gool AJ, Heidegger I, Ioannidis JPA, Jankowski J, Jankowski V, Jeronimo C, Kamat AM, Masereeuw R, Mayer G, Mischak H, Ortiz A, Remuzzi G, Rossing P, Schanstra JP, Schmitz-Dräger BJ, Spasovski G, Staessen JA, Stamatialis D, Stenvinkel P, Wanner C, Williams SB, Zannad F, Zoccali C, Vanholder R. Data Sharing Under the General Data Protection Regulation: Time to Harmonize Law and Research Ethics? Hypertension. Lippincott Williams and Wilkins; 2021. p. 1029–1035. PMID:33583200

68. Becker R, Chokoshvili D, Dove ES. Legal bases for effective secondary use of health and genetic data in the EU: time for new legislative solutions to better harmonize data for cross-border sharing? Int Data Priv Law. Oxford University Press; 2024. p. 223–246. doi: 10.1093/idpl/ipae014
69. HealthData@EU. Available from: https://acceptance.data.health.europa.eu/healthdata-central-platform/home?locale=en [accessed Dec 26, 2025]

Abbreviations

AI: Artificial Intelligence
DID / DIDs: Decentralized Identifier(s)
DLT: Distributed Ledger Technology
EHR / EHRs: Electronic Health Record(s)
EHDS: European Health Data Space
EMR: Electronic Medical Record
EUDI: European Digital Identity
FHIR: Fast Healthcare Interoperability Resources
GDPR: General Data Protection Regulation
HIE: Health Information Exchange
IoT: Internet of Things
IPFS: InterPlanetary File System
NFT / NFTs: Non-Fungible Token(s)
PHR / PHRs: Personal Health Record(s)
PICOS: Population, Intervention, Comparison, Outcome, and Study type
PRISMA: Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SUS: System Usability Scale
VC / VCs: Verifiable Credential(s)
ZKP / ZKPs: Zero-Knowledge Proof(s)