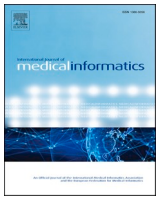
International Journal of Medical Informatics 214 (2026) 106405



Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.elsevier.com/locate/ijmedinf



Research Paper



HL7 FHIR consent for healthcare data sharing: challenges, opportunities and integrity implications

Sudip Phuyal [a], Manila Bhandari [a], Rabindra Bista [b], João Carlos Ferreira [a,c,d,*]

[a] Information Sciences, Technology and Architecture Research Centre (ISTAR), University Institute of Lisbon, (ISCTE-IUL), 1649-026 Lisbon, Portugal
[b] Department of Computer Science and Engineering, Kathmandu University, Dhulikhel 45200, Nepal
[c] Faculty of Logistics, Molde University College, 6410 Molde, Norway
[d] Inov Inesc Inovação – Instituto de Novas Tecnologias, 1000-029 Lisbon, Portugal

ARTICLE INFO

Keywords:
HL7 FHIR
Consent management
Healthcare data sharing
Interoperability
European Health Data Space
GDPR
Auditability
Governance
Blockchain
Integrity Anchoring

ABSTRACT

Objective: To assess whether HL7 FHIR Consent, as currently specified and deployed, is sufficient to support verifiable, regulation-aligned consent governance in distributed and cross-organisational health data sharing.
Methods: We conducted a qualitative critical analysis of FHIR Consent informed by (i) peer-reviewed implementation literature, (ii) national-scale consent exchange initiatives, and (iii) accountability requirements under GDPR and the European Health Data Space (EHDS). The analysis is organized into four dimensions: semantic interpretability, consent lifecycle management, runtime enforcement, and cross-organisational trust/auditability.
Results: FHIR Consent provides an interoperable representation of authorisation intent, but large-scale deployments remain limited by (1) non-canonical semantics across implementations, (2) lack of standardized lifecycle versioning and cross-organisational revocation propagation, (3) heterogeneous translation of declarative consent into enforceable access control, and (4) limited capability for independent verification of consent provenance and historical integrity across institutional boundaries.
Conclusion: We derive an architecture pattern that separates (a) standards-based consent representation (FHIR Consent), (b) local policy interpretation/enforcement, and (c) cross-organisational integrity verification. Cryptographic integrity anchoring is discussed as a complementary mechanism for tamper-evident verification of off-chain consent artifacts and lifecycle events, without externalizing consent semantics or personal data.

1. Introduction

The secure and accountable sharing of healthcare data is increasingly dependent on interoperable infrastructures that operate across organisational, institutional, and national boundaries. The expansion of multi-institutional clinical care, biomedical research collaboration, and cross-border health data reuse has intensified the need for governance mechanisms capable of ensuring that personal health information is accessed and processed in accordance with valid patient authorisation [1,2]. In such distributed environments, patient consent is not only a legal prerequisite but a core governance instrument that defines the legitimacy, scope, and duration of data access for both primary and secondary uses [3].

Regulatory developments further reinforce this requirement. Under the General Data Protection Regulation (GDPR) [4], consent must be demonstrable, revocable, and enforceable, and data controllers must be able to show that data processing was authorized at the time it occurred. Emerging sector-specific frameworks such as the European Health Data Space (EHDS) [5] extend these expectations by introducing harmonized mechanisms for cross-border health data use and enforceable individual rights, including opt-out from secondary use. Together, these frameworks shift attention from static consent documentation toward dynamic, verifiable, and interoperable consent governance across distributed infrastructures [6].

Within this context, HL7 FHIR [7] has become the dominant standard for healthcare data exchange. The FHIR Consent resource provides a structured and machine-interpretable representation of authorisation for data processing activities, enabling consent information to be exchanged across heterogeneous systems in a standardized format. This capability has positioned FHIR Consent as a foundational component of

* Corresponding author at: Information Sciences, Technology and Architecture Research Centre (ISTAR), University Institute of Lisbon, (ISCTE-IUL), 1649-026 Lisbon, Portugal.
E-mail address: jcafa@iscte-iul.pt (J.C. Ferreira).

https://doi.org/10.1016/j.ijmedinf.2026.106405
Received 16 February 2026; Received in revised form 11 March 2026; Accepted 16 March 2026
Available online 27 March 2026
1386-5056/© 2026 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

many contemporary health information exchange and research data sharing initiatives.

However, operational experience and implementation research indicate that representing consent in a standardized format does not, by itself, ensure consistent interpretation, enforceability, or verifiable accountability across organisational boundaries. Distributed ledger–based consent registries have therefore been proposed to provide tamper-evident and cross-organisationally verifiable consent management while preserving standards-based interoperability [8]. Consent is inherently dynamic, subject to modification and revocation over time, and must be interpreted and enforced within locally governed systems that may not share common trust assumptions or verification mechanisms. As healthcare data sharing becomes increasingly federated, the ability to independently verify consent validity, lifecycle history, and integrity across institutions emerges as a critical governance challenge.

This study critically analyses the role of HL7 FHIR Consent in distributed healthcare data sharing environments, focusing on governance limitations that emerge when consent must be interpreted, updated, and enforced across independent organisations. The analysis examines four dimensions: semantic interpretation across heterogeneous systems, consent lifecycle management and revocation, enforcement heterogeneity in runtime authorisation, and cross-organisational trust and auditability. Based on this structured evaluation, the paper derives standards-aligned architectural implications that preserve HL7 FHIR Consent as the authoritative and interoperable authorisation artefact while enabling stronger evidentiary assurance for consent lifecycle events and historical integrity in federated infrastructures. By clarifying the boundaries between consent representation, local enforcement, and independent integrity verification, the work provides a governance-oriented perspective on designing interoperable consent management for large-scale and cross-border healthcare data sharing.

2. Background and related work

HL7 FHIR has emerged as a widely adopted standard for healthcare data exchange, designed to enable interoperability through modular data structures, web-based interfaces, and extensible profiling mechanisms. Among its governance-related resources, the FHIR Consent resource provides a structured representation of an individual's authorisation or refusal for specific data processing activities [9]. Consent directives may be scoped by purpose of use, actors, data categories, and temporal validity, allowing complex authorisation conditions to be expressed in machine-interpretable form. FHIR-based consent models enable structured and machine-interpretable representation of authorisation rules, supporting integration with clinical systems and automated policy enforcement [10]. This design positions FHIR Consent as a standardized representation layer rather than an enforcement mechanism, with interpretation and access control delegated to surrounding system architectures.

It should also be noted that the HL7 FHIR Consent resource currently remains at Maturity Level 2 (Trial Use) within the HL7 FHIR development framework. As a result, operational implementations frequently depend on regional implementation guides and interoperability profiles that provide additional constraints and semantic alignment. For example, in the United States ecosystem, implementation often relies on frameworks such as US Core and related profiles, while other regions may define alternative governance and interoperability specifications. Consequently, interpretations of FHIR Consent behaviour may vary across implementation environments, and cross-regional comparisons must account for differences in implementation maturity and governance frameworks.

Prior research has demonstrated that FHIR-based consent representations can support interoperable exchange in large-scale healthcare infrastructures. National initiatives such as the German Medical Informatics Initiative have shown that modular informed consent templates can be implemented using HL7 FHIR profiles and shared semantic frameworks, enabling harmonized consent exchange across multiple university hospitals [11]. Similarly, large-scale deployments integrating consent management platforms with FHIR interfaces demonstrate that standardized consent information can be exchanged and validated across distributed clinical and research environments [12]. These implementations confirm that FHIR Consent is sufficiently expressive to model complex legal and ethical authorisation requirements when supported by coordinated governance and semantic alignment.

However, the literature consistently highlights limitations that extend beyond syntactic interoperability. Consent is inherently dynamic and must be managed across its lifecycle, including creation, modification, and withdrawal. Digital consent management frameworks emphasize the need for structured, reusable, and scalable mechanisms capable of handling heterogeneous research contexts and regulatory obligations [13]. Yet, current FHIR-based implementations frequently rely on centralized trusted components to maintain lifecycle consistency and enforce authorisation decisions, reflecting persistent dependence on institutional trust models [12].

Recent work on consent management for patient-generated health data further illustrates these challenges. While FHIR can serve as a unifying data exchange format supporting patient control and data sharing across organisations, consistent governance of access permissions and enforcement across distributed health data environments remains difficult due to fragmented data ownership, heterogeneous infrastructures and the need for coordinated policy enforcement across independent organisations [14]. Across these studies, interoperability and trust are typically addressed through local governance arrangements rather than through mechanisms that enable independent verification of consent integrity or historical validity across organisational boundaries.

Taken together, existing research demonstrates that HL7 FHIR Consent provides a robust and interoperable representation of authorisation but offers limited support for cross-organisational auditability, lifecycle verification, and independent trust establishment. These unresolved governance challenges motivate the need for architectural approaches that preserve standards-based consent representation while strengthening accountability and verifiability in distributed healthcare data sharing environments.

3. Research methodology

This study adopts a qualitative critical analysis approach to examine the governance implications of HL7 FHIR Consent in distributed healthcare data sharing environments. Rather than evaluating a specific technical implementation, the research focuses on analysing structural properties, design assumptions, and operational limitations of the FHIR Consent resource as reported in peer-reviewed literature, documented large-scale deployments, and regulatory frameworks governing healthcare data processing.

The analysis synthesizes evidence from implementation studies of FHIR-based consent exchange, digital consent management infrastructures, and policy guidance associated with data protection and secondary use of health data. These sources were examined to identify recurring challenges observed in real-world multi-organisational contexts, particularly those involving cross-institutional data exchange and federated governance models.

To structure the evaluation, the study analyses HL7 FHIR Consent across four analytical dimensions derived from implementation experience and regulatory accountability requirements. Semantic interpretability examines the consistency with which consent directives can be represented and understood across systems. Consent lifecycle management evaluates how creation, modification, and revocation of consent are represented and propagated over time. Enforcement feasibility considers how declarative consent directives are translated into runtime authorisation decisions within heterogeneous infrastructures. Cross-organisational trust and auditability assess the ability of independent

actors to verify consent validity, provenance, and historical integrity beyond institutional boundaries.

Based on this structured analysis, the study derives architectural implications that clarify how governance-critical requirements may be supported while preserving HL7 FHIR Consent as the authoritative standards-compliant representation of patient authorisation.

4. Findings: Governance challenges in HL7 FHIR consent

4.1. Semantic interpretability across heterogeneous systems

The HL7 FHIR Consent resource is designed to provide a flexible and expressive representation of authorisation conditions, enabling consent directives to be scoped by purpose of use, actors, data categories, and temporal validity. Efforts to formalize consent semantics through structured frameworks and computable FHIR models illustrate the importance of standardized consent interpretation for interoperability [10]. This flexibility supports the modelling of diverse legal and organisational requirements, but it also introduces interpretative variability across implementations. The FHIR specification deliberately avoids prescribing a canonical interpretation model for consent provisions, allowing implementers to adapt semantics to local governance contexts.

In practice, consistent interpretation often depends on shared implementation guides, code systems, and coordinated governance agreements. While such alignment is achievable within tightly governed networks, cross-organisational and cross-border data sharing environments frequently lack unified semantic constraints. As a result, identical consent structures may be interpreted differently by independent systems, particularly when translating complex legal or institutional rules into machine-readable form. This variability does not undermine syntactic interoperability but limits semantic consistency, creating uncertainty regarding how consent directives should be applied across heterogeneous infrastructures.

4.2. Consent lifecycle management and revocation

Consent is inherently dynamic and may be created, modified, or withdrawn over time. Although the FHIR Consent resource includes attributes that represent status and temporal validity, it does not define standardized mechanisms for lifecycle versioning, historical linkage, or propagation of consent changes across distributed systems. In multi-organisational environments, downstream systems must reliably recognize updated consent states to ensure that data access remains consistent with current authorisation.

Operational implementations frequently address this challenge through centralized registries or trusted intermediaries responsible for maintaining authoritative consent records and distributing updates. While such approaches support lifecycle coordination within bounded networks, they reintroduce centralized trust dependencies that may be difficult to sustain in federated or cross-border data sharing scenarios. Furthermore, demonstrating that consent was valid at a specific point in time requires reliable preservation of historical consent states and assurance that these records have not been altered retrospectively. Conventional database-based approaches, when managed independently across multiple institutions, provide limited guarantees of the historical integrity of consent artifacts.

4.3. Enforcement heterogeneity and runtime authorisation

HL7 FHIR Consent functions as a declarative representation of authorisation intent rather than an executable access control mechanism. Translating consent directives into runtime authorisation decisions requires integration with external enforcement components, such as role-based or attribute-based access control frameworks. Because FHIR does not prescribe how consent rules should be evaluated or enforced, implementation practices vary widely across organisations.

This heterogeneity introduces challenges for consistent governance in distributed data sharing environments. Authorisation decisions may be evaluated at different system layers, interpreted through different policy models, or influenced by organisation-specific governance rules. When health data are aggregated, transformed, or reused across institutional boundaries, variations in enforcement logic may result in inconsistent application of consent directives. While such flexibility reflects the design philosophy of FHIR and supports local autonomy, it complicates the establishment of predictable and harmonized authorisation behaviour across federated infrastructures.

4.4. Cross-Organisational trust and auditability

Distributed healthcare data sharing requires participants to trust not only the content of consent records but also their integrity, provenance, and lifecycle history. Standard FHIR-based exchanges typically assume trust in the originating system that provides consent information. In loosely coupled or cross-border environments, however, such trust assumptions may not be sufficient, particularly when organisations operate under independent governance frameworks and regulatory jurisdictions.

Existing implementations often rely on institutional audit logs, centralized registries, or trusted intermediaries to support accountability [8]. While effective within coordinated governance networks, these mechanisms provide limited support for independent verification of consent integrity across organisational boundaries. Verifying that a consent record has not been modified after creation, or that a revocation was applied consistently across systems, remains difficult when records are stored and managed by multiple independent entities. This limitation is particularly significant in regulatory contexts that require demonstrable accountability, retrospective auditing, and dispute resolution over extended time periods.

4.5. Synthesis of governance challenges

Taken together, these findings indicate that the primary challenges associated with HL7 FHIR Consent in distributed healthcare data sharing are governance-related rather than purely technical. The standard provides a robust and interoperable representation of authorisation, but it does not define mechanisms for ensuring consistent interpretation, coordinated lifecycle management, harmonized enforcement, or independently verifiable trust across organisational boundaries. These functions are delegated to surrounding governance structures and system architectures, which vary widely in practice.

As healthcare data sharing becomes increasingly federated and subject to stringent regulatory accountability requirements, the separation between consent representation, enforcement, and trust verification becomes more consequential. Addressing this separation does not require replacing HL7 FHIR Consent, but it does necessitate architectural approaches that complement standards-based interoperability with mechanisms capable of supporting verifiable lifecycle management and cross-organisational accountability.

5. Architectural implications for consent governance

The governance challenges identified in the preceding analysis do not arise from deficiencies in the HL7 FHIR Consent resource itself, but from the structural separation between consent representation, enforcement behaviour, and trust establishment in distributed healthcare data sharing environments. Addressing these challenges therefore requires architectural approaches that complement standards-based consent representation with mechanisms that support lifecycle verification and cross-organisational accountability without altering the normative semantics of FHIR Consent.

A central implication of the analysis is the need to explicitly separate

three governance responsibilities: authoritative consent representation, local interpretation and enforcement, and cross-organisational integrity verification. Fig. 1 illustrates the conceptual separation of consent representation, enforcement, and cross-organisational verification derived from this analysis.

This separation preserves HL7 FHIR Consent as the authoritative authorisation artifact while enabling independent verification of consent lifecycle integrity across organisational boundaries. HL7 FHIR Consent can continue to function as the authoritative representation of patient authorisation, stored and managed within FHIR-compliant repositories under the control of data controllers. This preserves interoperability, standards compliance, and regulatory flexibility, including the ability to modify or withdraw consent over time.

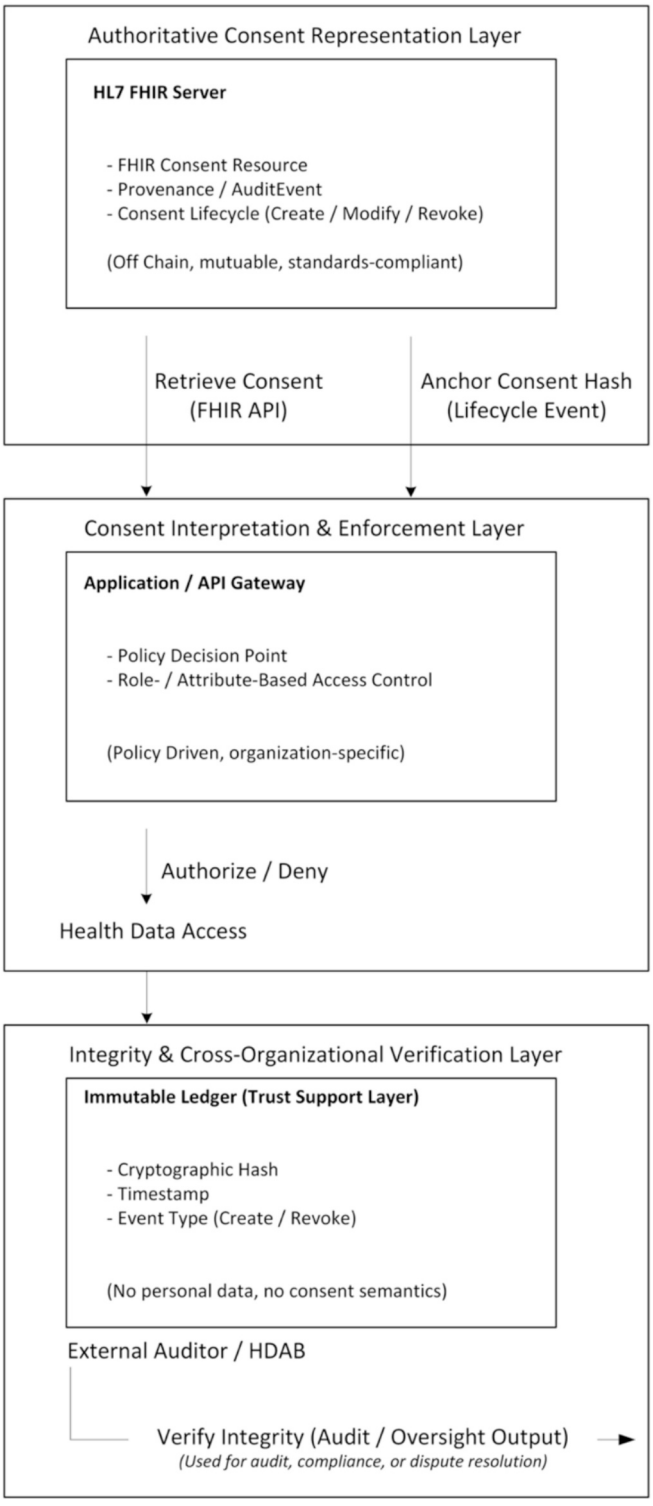


Fig. 1. Conceptual governance architecture for HL7 FHIR consent in distributed healthcare data sharing.

Authorisation decisions, however, remain operationally dependent on local policy interpretation and enforcement mechanisms. Because HL7 FHIR Consent is intentionally declarative, runtime authorisation must be performed by organisation-specific access control components that translate consent directives into actionable policies. The analysis indicates that such enforcement heterogeneity is an inherent characteristic of distributed data sharing and cannot be fully eliminated through standardization of consent representation alone. Instead, architectural clarity is required to distinguish between representation and enforcement as separate governance functions.

A further implication concerns the establishment of verifiable trust across organisational boundaries. While FHIR-based exchanges enable interoperable sharing of consent information, they do not provide mechanisms for independent verification of consent integrity or lifecycle history. To support auditability and cross-organisational accountability, complementary mechanisms are required that enable tamper-evident verification of consent artifacts without embedding consent semantics or personal data outside the FHIR ecosystem.

One approach consistent with these requirements is cryptographic integrity anchoring. Prior architectural models have explored recording consent transactions or smart contract states on distributed ledgers while retaining FHIR-based consent resources off-chain for operational use [8]. In this model, HL7 FHIR Consent resources remain stored off-chain within institutional repositories, while cryptographic hashes representing consent states or lifecycle events are anchored in an immutable ledger. This process does not create an alternative consent representation or enforcement layer. Instead, it provides a verifiable reference that can be used to confirm that a consent record existed at a given point in time and has not been altered retrospectively. Because only non-interpretable cryptographic references are anchored, regulatory principles such as data minimization and consent revocability remain unaffected.

Fig. 1 illustrates this conceptual separation of governance responsibilities. Consent representation remains standards-based and mutable, enforcement remains locally governed, and integrity anchoring functions as an independent verification mechanism supporting cross-organisational trust. By decoupling these functions, distributed healthcare data sharing infrastructures can strengthen accountability and auditability while preserving HL7 FHIR Consent as the authoritative and interoperable representation of patient authorisation.

For illustration, consider a cross-border EHDS scenario in which a German university hospital creates and stores a patient's FHIR Consent resource (including revocation events). When a French research institution later requests access, it retrieves the FHIR Consent via standard REST API, interprets and enforces it through its local policy engine, and independently verifies the integrity and historical validity of consent creation/revocation events through the cryptographic anchor published on a shared ledger. This approach preserves full HL7 FHIR interoperability and local autonomy while providing tamper-evident, cross-organisational accountability, exactly the separation of responsibilities proposed in this architecture.

6. Discussion

The analysis presented in this study clarifies the role of HL7 FHIR Consent within contemporary healthcare data sharing ecosystems. FHIR Consent provides a standardized and interoperable representation of authorisation, but it does not function as a comprehensive governance mechanism on its own. The findings demonstrate that challenges related to semantic consistency, lifecycle coordination, enforcement, and trust

arise not from deficiencies in the standard, but from the broader socio-technical context in which consent is interpreted and applied. In distributed and cross-organisational environments, representation, enforcement, and verification operate under different governance structures and trust assumptions, creating a structural separation that must be addressed architecturally rather than purely through data standardization.

This distinction becomes particularly significant in the context of evolving regulatory frameworks governing healthcare data exchange. In particular, the General Data Protection Regulation (GDPR) and the emerging European Health Data Space (EHDS) place increasing emphasis on demonstrable accountability, verifiable authorisation, and cross-border interoperability for health data processing. Under the General Data Protection Regulation, organisations must be able to demonstrate that data processing was authorized at the time it occurred and that consent withdrawal is respected without undue delay. The European Health Data Space further extends these expectations by introducing cross-border governance mechanisms and enforceable individual rights related to secondary use of health data. Together, these frameworks emphasize accountability and verifiability over static documentation, requiring healthcare data sharing infrastructures to support demonstrable consent lifecycle management across institutional boundaries. The findings suggest that syntactic interoperability alone is insufficient to meet these governance requirements when consent records are created, interpreted, and enforced by independent actors. Table 1 summarizes the relationship between key governance requirements in distributed healthcare data sharing, the capabilities of HL7 FHIR Consent, and the architectural implications derived from this analysis.

This synthesis highlights that governance challenges arise primarily from the separation between representation, enforcement, and verification rather than from limitations of the FHIR standard itself. The architectural implications proposed in this study reflect an attempt to reconcile standards-based interoperability with governance-driven accountability. By preserving HL7 FHIR Consent as the authoritative representation of authorisation while introducing complementary mechanisms for integrity verification, consent management can remain aligned with existing healthcare interoperability frameworks while supporting independent auditability. In this context, cryptographic integrity anchoring should be understood as a supporting trust mechanism rather than a replacement for institutional governance or policy enforcement. Its value lies in enabling tamper-evident verification of consent artifacts and lifecycle events, thereby strengthening evidentiary assurance in federated environments without embedding consent semantics in distributed ledgers.

Table 1
Governance requirements, HL7 FHIR consent capabilities and architectural implications.

Governance requirement	HL7 FHIR Consent capability	Governance limitation	Architectural implication
Consent revocation and lifecycle management	Status and temporal validity attributes	No standardized cross-organisational lifecycle coordination	Verifiable lifecycle tracking through integrity anchoring
Demonstrable authorisation over time	Representation of validity periods and consent states	Limited guarantees of historical integrity across systems	Tamper-evident verification of consent history
Accountability and auditability	Provenance and audit-related resources	Trust dependent on institutional control	Independent cross-organisational verification
Federated and cross-border data sharing	Interoperable consent representation	Implicit trust assumptions between data holders	Decoupled trust verification mechanisms

At the same time, the analysis highlights the limits of technological solutions. Integrity anchoring does not resolve semantic ambiguity in consent interpretation, nor does it standardize enforcement behaviour across organisations. Authorisation decisions remain shaped by local policy frameworks, institutional governance arrangements, and regulatory interpretation. Consequently, achieving consistent consent governance in distributed healthcare data sharing environments requires coordination at both technical and organisational levels, including shared semantic frameworks, profiling strategies, and governance agreements.

This study has several limitations. The analysis is conceptual and based on synthesis of existing literature, documented implementation experience, and regulatory requirements rather than empirical evaluation of a specific system. In addition, the HL7 FHIR Consent resource currently remains at Maturity Level 2 (Trial Use). Operational implementations are frequently shaped by regional implementation guides and profiles (for example, US Core in the United States ecosystem), which may introduce interpretation differences across jurisdictions. Consequently, while the manuscript references European regulatory frameworks such as GDPR and the EHDS, direct comparisons should be interpreted cautiously because implementation maturity and governance models are not yet fully harmonised internationally.

Despite these limitations, the study provides a structured perspective on how standards-based consent representation and verifiable accountability mechanisms may be combined to support trustworthy and interoperable healthcare data sharing at scale.

7. Conclusion

This study examined the role of HL7 FHIR Consent in distributed healthcare data sharing environments from a governance-oriented perspective. While the FHIR Consent resource provides a standardized and expressive representation of patient authorisation, the analysis demonstrated that practical implementations face persistent challenges related to semantic interpretation, consent lifecycle coordination, enforcement consistency, and cross-organisational trust. These challenges do not stem from limitations of the standard itself, but from the structural separation between consent representation, operational enforcement, and trust verification in federated data sharing ecosystems.

To address this separation, the study derived architectural implications that preserve HL7 FHIR Consent as the authoritative standards-based representation of authorisation while introducing complementary mechanisms for verifiable lifecycle management and independent auditability. In particular, cryptographic integrity anchoring was examined as a supporting mechanism for tamper-evident verification of consent artifacts and historical states without embedding consent semantics or personal data outside established interoperability frameworks. This standards-aligned approach enables stronger accountability and cross-organisational trust while maintaining regulatory flexibility and interoperability. As healthcare data ecosystems become increasingly federated and cross-border in nature, such governance-oriented architectures will become critical for ensuring trustworthy and compliant health data exchange.

Overall, the findings highlight that effective consent governance in distributed healthcare data sharing requires coordination between interoperable data standards and mechanisms that support demonstrable accountability across institutional boundaries. Future work should focus on empirical evaluation of governance architectures in operational healthcare data sharing environments, including pilot implementations that integrate HL7 FHIR Consent with mechanisms for verifiable lifecycle management and cross-organisational accountability.

CRediT authorship contribution statement

Sudip Phuyal: Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Manila Bhandari:** Writing – review & editing, Writing – original draft, Formal analysis, Data curation, Conceptualization. **Rabindra Bista:** Writing – review & editing, Visualization, Supervision. **João Carlos Ferreira:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Project administration, Investigation.

Funding

This work is funded by national funds through FCT - Fundacao para a Ciencia e a Tecnologia, I.P., under projects/supports UID/6486/2025 (https://doi.org/10.54499/UID/06486/2025) and UID/PRR/6486/2025 (https://doi.org/10.54499/UID/PRR/06486/2025).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] C.N. Vorisek, M. Lehne, S.A.I. Klopfenstein, P.J. Mayer, A. Bartschke, T. Haese, S. Thun, Fast Healthcare Interoperability Resources (FHIR) for Interoperability in Health Research: Systematic Review, JMIR Med. Inform. 10 (2022) e35724, https://doi.org/10.2196/35724.

[2] S. Phuyal, L.B. Elvas, J.C. Ferreira, R. Bista, Blockchain Technology in Healthcare: Unifying Patient Medical Records - A Survey, in: V. Sakalauskas, A. Bajaj, A. Abraham, K.R. Madhavi, P. Manghirmalani Mishra (Eds.), Bio-Inspired Comput., Springer Nature Switzerland, Cham, 2025: pp. 319–332. Doi: 10.1007/978-3-031-78946-5_31.

[3] P. Lee, D. Mendoza, M. Kaiser, E. Lott, G. Singh, A. Grando, FHIR Granular Sensitive Data Segmentation, Appl. Clin. Inform. 16 (2025) 156–166, https://doi.org/10.1055/a-2466-4371.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), 2016. http://data.europa.eu/eli/reg/2016/679/oj (accessed November 3, 2025).

[5] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance), 2025. http://data.europa.eu/eli/reg/2025/327/oj/eng (accessed August 14, 2025).

[6] W.M. Charles, M.B. van der Waal, J. Flach, A. Bisschop, R.X. van der Waal, H. Es-Sbai, C.J. McLeod, Blockchain-based Dynamic Consent and its applications for Patient-Centric Research and Health Information Sharing: Protocol for an Integrative Review, JMIR Res. Protoc. 13 (2024), https://doi.org/10.2196/50339.

[7] FHIR Release 5 (R5), Version 5.0.0, Health Level Seven Int. HL7 (2023). https://www.hl7.org/fhir/ (accessed December 27, 2025).

[8] F. Oke, S.A. Adeniji, O. Bolaji, O. Dopamu, B.S. Ajibade, Blockchain-Enabled Consent Management in FHIR-Compliant Oncology Platforms, Authorea Prepr. (2025). https://www.techrxiv.org/doi/full/10.36227/techrxiv.174918103.37396756 (accessed February 16, 2026).

[9] FHIR Release 6 (R6) Ballot3 - Consent Resource, Health Level Seven Int. HL7 (n.d.). https://build.fhir.org/consent.html (accessed December 12, 2025).

[10] A. Voronov, M. Jafari, L. Zhao, M. Soliz, Q. Hong, J. Pope, D. Chern, M. Lipman, A. Grando, Pediatric Consent on FHIR, Appl. Clin. Inform. 15 (2024) 342–356, https://doi.org/10.1055/a-2291-1482.

[11] R. Bild, M. Bialke, K. Buckow, T. Ganslandt, K. Ihrig, R. Jahns, A. Merzweiler, S. Roschka, B. Schreiweis, S. Stäubert, S. Zenker, F. Prasser, Towards a comprehensive and interoperable representation of consent-based data usage permissions in the German medical informatics initiative, BMC Med. Inform. Decis. Mak. 20 (2020) 103, https://doi.org/10.1186/s12911-020-01138-6.

[12] M. Bialke, L. Geidel, C. Hampf, A. Blumentritt, P. Penndorf, R. Schuldt, F.-M. Moser, S. Lang, P. Werner, S. Stäubert, H. Hund, F. Albashiti, J. Gührer, H.-U. Prokosch, T. Bahls, W. Hoffmann, A FHIR has been lit on gICS: facilitating the standardised exchange of informed consent in a large network of university medicine, BMC Med. Inform. Decis. Mak. 22 (2022) 335, https://doi.org/10.1186/s12911-022-02081-4.

[13] M. Bialke, T. Bahls, L. Geidel, H. Rau, A. Blumentritt, S. Pasewald, R. Wolff, J. Steinmann, T. Bronsch, B. Bergh, G. Tremper, M. Lablans, F. Ückert, S. Lang, T. Idris, W. Hoffmann, MAGIC: once upon a time in consent management—a FHIR® tale, J. Transl. Med. 16 (2018) 256, https://doi.org/10.1186/s12967-018-1631-3.

[14] P. Randine, E. Salant, M. Muzny, L. Pape-Haugaard, Consent Management System on Patient-Generated Health Data, in: J. Bichel-Findlay, P. Otero, P. Scott, E. Huesing (Eds.), Stud. Health Technol. Inform., IOS Press, 2024. Doi: 10.3233/SHTI230956.