



HF-SECURE HEALTH: A HYPERLEDGER FABRIC-BASED PERMISSIONED BLOCKCHAIN FRAMEWORK FOR SECURE, PRIVACY-PRESERVING HEALTHCARE DATA MANAGEMENT

J. P. Keerthana* & S. Jayaprakash**

* Research Scholar in Computer Science, Edayathangudy G.S. Pillay Arts & Science College (A),
Nagapattinam, Tamil Nadu, India

** Research Supervisor in Computer Science, Edayathangudy G.S. Pillay Arts & Science College (A),
Nagapattinam, Tamil Nadu, India

Cite This Article: J. P. Keerthana & S. Jayaprakash, "HF-Secure Health: A Hyperledger Fabric-Based Permissioned Blockchain Framework for Secure, Privacy-Preserving Healthcare Data Management", International Journal of Computational Research and Development, Volume 11, Issue 2, July - December, Page Number 3-9, 2026.

Copy Right: © DV Publication, 2026 (All Rights Reserved). This is an Open Access Article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium provided the original work is properly cited.

Type of Review: Peer Reviewed as per |C|O|P|E| Guidance.

Disclaimer: The scholarly papers reviewed and published by DV Publication, India, reflect the views and opinions of their respective authors and do not necessarily represent the views or opinions of DV Publication. The publisher disclaims any responsibility for any harm, loss, or damage resulting from the use of the published content by any party.

DOI: <https://doi.org/10.5281/zenodo.23087438>

Abstract:

Healthcare information systems increasingly rely on electronic health records (EHRs), clinical reports, diagnostic images, prescriptions, laboratory results, and connected medical devices. However, centralized architectures face challenges related to security, privacy, interoperability, and auditability. This paper proposes HF-Secure Health, a permissioned healthcare data-management framework based on Hyperledger Fabric. The framework stores encrypted clinical data in controlled off-chain storage while maintaining hashes, consent states, access policies, provenance, and transaction evidence on the blockchain ledger. A consortium network connects patients, hospitals, physicians, laboratories, pharmacies, and authorized research organizations. Fabric Membership Service Providers (MSPs), certificate-based identities, channels, private data mechanisms, and chaincode-based policies enable organizational separation and fine-grained authorization. Patient-centric consent management supports time-limited access, revocation, and immutable auditing. HL7 FHIR-aligned metadata improves interoperability with existing healthcare applications. The proposed methodology includes system architecture, transaction workflow, smart-contract logic, security analysis, threat modeling, and reproducible evaluation. Performance is assessed using transaction latency, throughput, storage overhead, unauthorized-access resistance, and audit completeness. The framework integrates blockchain, privacy, consent management, and interoperability for secure healthcare data sharing.

Key Words: Hyperledger Fabric; Healthcare Blockchain; EHR; Privacy; Access Control; Smart Contracts; Consent Management; Interoperability.

1. Introduction:

Healthcare organizations generate and exchange highly sensitive information across hospitals, clinics, laboratories, pharmacies, insurance providers, emergency services, and research institutions. EHRs improve clinical continuity, but the underlying information environment is commonly fragmented across institutional databases and applications. The resulting fragmentation can make it difficult to establish a consistent history of who created, accessed, changed, or shared a record. Blockchain has therefore attracted substantial research interest as a mechanism for maintaining a tamper-evident transaction history among organizations that do not want to place complete trust in a single data custodian [1-4].

A healthcare blockchain should not simply copy an entire medical database onto a distributed ledger. Medical records may contain large imaging files, laboratory documents, genomic information, and personally identifiable information. Replicating such content to every participant can increase storage cost and create privacy and governance problems. Earlier work has consequently explored hybrid on-chain/off-chain models in which the blockchain stores references, hashes, permissions, and provenance while the clinical payload remains in protected storage [5-7].

Hyperledger Fabric is particularly suitable for a healthcare consortium because it is a permissioned distributed-ledger platform rather than a public crypto currency network. Organizations can be identified through membership services, transactions can be governed by endorsement policies, and private communication can be supported through channels and private data collections. These characteristics are aligned with the need to restrict medical information to authorized participants while preserving a shared audit trail. Existing studies have demonstrated the feasibility of Fabric-based EHR architectures, but important research gaps remain in combining patient consent, interoperable metadata, fine-grained authorization, off-chain encrypted storage, and systematic security evaluation [8-10].

This paper proposes HF-Secure Health to address these gaps. The principal idea is to treat the blockchain as a trusted coordination and evidence layer rather than as a repository for raw medical files. A patient record is represented by a unique identifier, a FHIR-aligned metadata object, a cryptographic digest, an encrypted storage reference, a consent state, and provenance information. Chaincode controls the state transitions associated with record creation, access requests, approval, revocation, emergency access, and audit logging.

The contributions of this work are fourfold. First, a permissioned multi-organization Hyperledger Fabric architecture is designed for healthcare data sharing. Second, a patient-centric consent and role/attribute-based authorization model is integrated into chaincode. Third, a hybrid storage design protects large clinical objects while preserving on-chain integrity verification. Fourth, a reproducible evaluation methodology and threat model are defined so that performance and security claims can be validated experimentally rather than assumed.

The remainder of the paper is organized as follows. Section 2 discusses related research. Section 3 presents the problem statement and research objectives. Section 4 describes the proposed architecture. Section 5 explains the methodology and transaction workflows. Section 6 presents the chaincode algorithms. Section 7 describes security properties and threat analysis. Section 8 provides the implementation and evaluation plan. Section 9 discusses limitations. Section 10 concludes the paper.

2. Related Work:

Blockchain-based healthcare research can broadly be grouped into EHR management, patient-controlled health records, secure data sharing, privacy-preserving access control, and blockchain-enabled interoperability. Yue et al. proposed a healthcare data gateway in which blockchain supports patient control and secure sharing, highlighting the importance of privacy-aware access models [1]. Xia et al. introduced BBDS for blockchain-based sharing of electronic medical records in cloud environments, demonstrating the value of separating healthcare data management from conventional centralized trust assumptions [2].

FHIR Chain addressed interoperability by representing clinical information using the HL7 FHIR standard and recording verifiable references on a blockchain [3]. This approach is important because blockchain does not itself solve semantic interoperability; common data models and APIs are still required. Shen et al. proposed MedChain to support efficient healthcare information sharing and emphasized the need to handle multiple classes of healthcare information rather than treating all records as a single data type [4].

Guo et al.'s Ancile framework explored blockchain-supported privacy, access control, and interoperability for EHRs [5]. Mayer et al. conducted a systematic review of blockchain-based EHR research and identified recurring issues involving scalability, privacy, interoperability, and adoption [6]. Wu et al. proposed a privacy-preserved blockchain-based smart healthcare system for exchanging and sharing electronic medical records, demonstrating the importance of cryptographic privacy mechanisms in addition to ledger immutability [7].

Hyperledger Fabric-specific research has become increasingly relevant. Uddin et al. presented a Fabric architecture for EHRs using organizational peer nodes and channels to provide secure communication among healthcare stakeholders [8]. Ndzimakhwe et al. examined a user-focused EHR system leveraging Fabric and discussed customization requirements for practical healthcare adoption [9]. Hasnain et al. systematically reviewed Fabric's role in EHR security and identified the framework's permissioned architecture as an important advantage for healthcare environments [10].

These studies show that the field is moving from simple ledger storage toward integrated architectures that combine blockchain with cryptographic access mechanisms and external storage.

Despite this progress, three gaps remain. First, some designs describe access control but do not provide a complete consent lifecycle including grant, expiry, revocation, and emergency access. Second, interoperability is often mentioned without specifying how blockchain records map to standardized clinical resources. Third, many evaluations report transaction performance without simultaneously evaluating unauthorized-access resistance, audit completeness, and storage overhead. HF-Secure Health addresses these gaps through an integrated design.

3. Problem Statement and Objectives:

The central problem addressed in this study is the secure exchange of healthcare information among mutually independent organizations without creating a new centralized repository that becomes a single point of failure or control. The solution must preserve confidentiality, integrity, availability, accountability, and patient privacy while remaining usable by clinical and administrative stakeholders.

The specific objectives are:

- to create a permissioned blockchain network for healthcare consortium members
- to establish cryptographically verifiable identities for patients and providers
- to support patient-controlled consent and organizational authorization
- to maintain tamper-evident records of creation and access events
- to keep large medical payloads outside the ledger while anchoring their integrity on-chain
- to support interoperable metadata using FHIR-aligned structures and
- to define measurable performance and security experiments

4. Proposed HF-Secure Health Architecture:

HF-Secure Health consists of five logical layers: the application layer, identity and access layer, blockchain network layer, secure storage layer, and interoperability layer. The application layer provides interfaces for patients, clinicians, laboratories, pharmacies, administrators, and researchers. The identity layer manages digital certificates and organizational membership. The blockchain layer maintains consent, metadata, transaction provenance, and audit events. The secure storage layer contains encrypted medical files. The interoperability layer converts application data into standardized FHIR-aligned metadata. The consortium contains six representative organizations: Patient Organization, Hospital A, Hospital B, Laboratory, Pharmacy, and Research Organization. In a practical deployment, these do not necessarily represent legal entities literally called organizations; they represent Fabric MSP domains controlled by participating institutions. Each organization operates one or more peers. An ordering service sequences transactions, and endorsement policies specify which organizations must approve a transaction before it is committed.

Raw medical data are not stored directly in the ledger. When a healthcare provider creates a report, the application encrypts the file using an approved encryption mechanism and places the ciphertext in controlled storage. A cryptographic hash is calculated over the encrypted object. The ledger stores the patient pseudonymous identifier, resource type, storage locator, hash, creator identity, timestamp, consent state, and access policy. When a user retrieves a file, the application checks authorization, obtains the encrypted object, recomputes the hash, and compares it with the ledger value before decryption.

The design uses three categories of blockchain state. Identity state records pseudonymous identities and organizational roles. Clinical metadata state records the existence and integrity information for each medical resource. Consent state records the

patient's authorization rules. Access events are appended as audit transactions. Because the ledger is append-oriented, a correction to a clinical record is represented as a new version rather than an in-place destructive modification as shown in table 1.

Table 1: Architectural Layers, Components and Functional Purposes of the HF-Secure Health Framework

Layer	Components	Purpose
Application	Patient portal, clinician portal, lab/pharmacy modules	Human-facing healthcare workflows
Identity & access	Fabric CA/MSP, certificates, roles, attributes	Authentication and authorization
Blockchain	Peers, ordering service, channels, chain code	Consensus, provenance, consent, audit
Secure storage	Encrypted DB/object store/IPFS-compatible repository	Large clinical payloads
Interoperability	FHIR-aligned JSON, REST/API gateway	Exchange with existing EHR systems

5. System Methodology:

The HF-Secure Health methodology provides a secure and patient-centric workflow for managing healthcare data using Hyperledger Fabric. It covers patient registration, encrypted medical record creation, consent-based access authorization, revocation, and controlled emergency access. Each transaction is validated through chaincode and recorded with immutable audit and provenance information. Medical records are maintained in encrypted off-chain storage, while hashes and essential metadata are stored on the blockchain as shown in figure 1. FHIR-aligned data representation enables interoperability with existing EHR systems while preserving privacy and minimizing blockchain storage requirements.

5.1 Patient Registration:

A patient first registers through an authorized healthcare identity service. The application verifies the registration evidence according to institutional policy and creates a pseudonymous blockchain identifier. Personally identifying attributes need not be placed in the shared ledger. The identity provider issues a certificate or application credential associated with the permitted role. The ledger records the patient's blockchain identity and status without exposing unnecessary personal information.

5.2 Medical Record Creation:

When a physician or laboratory creates a clinical resource, the application validates the resource schema, encrypts the payload, stores the ciphertext, calculates a cryptographic digest, and submits a Create Record transaction. Chaincode checks that the submitting identity has a permitted clinical role, that the patient exists, and that required metadata are present. The transaction then records the resource reference and hash. The resulting ledger entry provides evidence that a particular encrypted object existed in the stated form at the time of commitment.

5.3 Consent Grant:

The patient or legally authorized representative can grant access to a provider, organization, or role. A consent object contains the patient pseudonymous identifier, grantee identifier, permitted resource category, purpose, start time, expiry time, and status. Chaincode validates the request and records the consent. Time limits are important because indefinite access increases the impact of credential compromise.



Figure 1: HF-Secure Health System Cycle

5.4 Access Request and Authorization:

A clinician requests access through the application. The request is transformed into an Access Request transaction containing the resource identifier and intended purpose. Chaincode evaluates the caller's certificate attributes, organizational membership, active consent, resource policy, and temporal constraints. If all conditions are satisfied, the transaction returns an authorization decision and creates an audit record. The application then retrieves the encrypted object from off-chain storage.

5.5 Consent Revocation:

Revocation changes the state of the corresponding consent record to revoked and records the actor and time. Future access attempts fail the chaincode authorization check. Revocation cannot guarantee that a previously authorized recipient has destroyed a copy obtained earlier; therefore, governance policies and technical controls outside the ledger remain necessary.

5.6 Emergency Access:

Healthcare systems require emergency or break-glass access in situations where the patient cannot provide normal consent. HF-Secure Health permits an emergency role to request access only when the requester provides a documented reason

and the transaction is endorsed according to a stronger policy. Emergency events are flagged in the audit trail and can trigger retrospective review by a privacy officer. The design intentionally does not treat emergency access as unrestricted access.

5.7 Record Versioning and Integrity Verification:

Medical information can legitimately change because new laboratory results, corrections, diagnoses, and follow-up notes are added. Instead of modifying an existing ledger object destructively, each version receives a unique version identifier and a parent-record reference. The system can therefore reconstruct the provenance chain. During retrieval, the stored ciphertext is hashed again and compared with the committed digest.

5.8 Interoperability:

The interoperability layer represents common healthcare entities using FHIR-aligned concepts such as Patient, Observation, Diagnostic Report, Medication Request, Encounter, and Document Reference. The blockchain does not need to contain every FHIR field. Instead, the ledger anchors a minimal metadata representation and a reference to the encrypted FHIR document. This approach reduces ledger size and permits existing EHR systems to continue using standard APIs.

6. Chaincode and Algorithms:

The chaincode acts as the policy enforcement layer. It should implement deterministic state transitions and avoid storing secrets or large clinical objects. Representative functions include Register Patient (), Create Record (), Request Access (), Grant Consent (), Revoke Consent (), Verify Access (), Record Emergency Access (), and Verify Integrity ().

Algorithm 1: Secure Medical Record Registration

Input: patient ID, resource Type, encrypted Object, metadata, creator Identity. Output: committed record ID.

Step 1: authenticate creator Identity through Fabric credentials.

Step 2: verify that creator has a permitted role.

Step 3: encrypt and store the clinical object outside the ledger.

Step 4: calculate $H = \text{Hash}(\text{encrypted Object})$.

Step 5: generate unique record ID and version ID.

Step 6: submit transaction containing patient ID, resource Type, storage URI, H , creator, timestamp, and policy metadata. Step 7: obtain required endorsements.

Step 8: commit the transaction.

Step 9: return record ID.

Algorithm 2: Consent-Based Access

Input: requester ID, record ID, purpose. Output: ALLOW or DENY.

Step 1: authenticate requester.

Step 2: obtain requester organization and role attributes.

Step 3: load record policy.

Step 4: load active patient consent.

Step 5: verify that current time is within the consent interval.

Step 6: verify resource and purpose constraints.

Step 7: if every predicate is true, return ALLOW and append an audit transaction; otherwise return DENY and append a denied-access event.

Algorithm 3: Integrity Verification

Input: record ID. Output: VERIFIED or TAMPERED.

Step 1: retrieve the ledger digest H .

Step 2: retrieve encrypted object from the storage locator.

Step 3: calculate $H' = \text{Hash}(\text{encrypted Object})$.

Step 4: compare H and H' .

Step 5: return VERIFIED if $H = H'$; otherwise return TAMPERED and create a security event.

The principal security property is that a storage compromise cannot silently modify a medical object without changing its digest. The ledger therefore acts as an integrity anchor. However, a hash does not provide confidentiality; encryption and storage access controls are still required.

7. Security and Threat Analysis:

The threat model considers external attackers, compromised user credentials, malicious insiders, unauthorized healthcare workers, storage tampering, replay attempts, and collusion among a limited number of consortium members. The framework assumes that the underlying cryptographic primitives and Fabric membership infrastructure are correctly configured as shown in table 2. It does not assume that every healthcare organization is honest.

Confidentiality is achieved primarily through encryption, private data mechanisms, application authorization, and storage controls. Integrity is supported by cryptographic hashes and the append-oriented ledger. Authentication relies on Fabric's identity framework. Authorization is multi-factor in the policy sense: organizational identity, role/attributes, patient consent, resource type, purpose, and time constraints are jointly evaluated. Accountability is provided by signed transactions and immutable audit history.

Table 2: Threat Model, Attack Vectors, Security Controls, and Residual Risks of HF-Secure Health

Threat	Attack vector	HF-Secure Health control	Residual risk
Unauthorized access	Stolen provider credentials	Certificate identity + role/attribute + consent check	Credential theft requires revocation and monitoring
Record tampering	Modification of off-chain file	Hash anchored on ledger	Attacker may replace both storage and trusted application components
Insider misuse	Legitimate user accesses unrelated records	Purpose/resource policy + audit trail	Organizational enforcement remains necessary

Replay	Reuse of old access request	Unique transaction IDs and state checks	Application-level nonce/session controls should be added
Data leakage	Exposure of raw ledger data	No raw clinical payload on shared ledger	Metadata can still reveal patterns
Node failure	Peer unavailable	Multiple peers and ordered ledger replication	Network capacity must be engineered
Collusion	Several organizations cooperate maliciously	Endorsement policies and governance	Consortium governance remains essential
Emergency abuse	Break-glass role misused	Reason capture + stronger endorsement + review	Human oversight required

Privacy requires special attention because immutability can conflict with requirements to correct or erase personal information. The proposed design minimizes this conflict by avoiding raw personal health data on the ledger. Pseudonymous identifiers and hashes are used for ledger state, while the authoritative encrypted payload is held in controlled storage. A production deployment must still conduct a jurisdiction-specific legal and privacy assessment before claiming compliance with a particular regulation.

8. Implementation and Evaluation Methodology:

The framework can be implemented using a current supported Hyperledger Fabric release, Docker-based deployment, Fabric Certificate Authorities, a CouchDB state database, a Node.js or Go chaincode implementation, and a REST/SDK application layer. A minimum experimental consortium may contain four organizations: Hospital A, Hospital B, Laboratory, and Pharmacy. A fifth organization can represent the patient identity service. Each organization can operate one peer, while the ordering service can be deployed with multiple nodes for fault tolerance as shown in table 3.

A reproducible dataset should be generated rather than using identifiable patient records. Each synthetic patient can be assigned multiple resource types including demographics, encounter summaries, observations, diagnostic reports, prescriptions, and laboratory results. Record sizes can be varied to represent text, structured JSON, PDF documents, and imaging references. Access requests should include both legitimate and unauthorized scenarios.

Table 3: Experimental Configuration and Performance Evaluation Metrics

Experiment	Independent variable	Dependent metrics
Transaction load	100-10,000 transactions	Throughput, latency, failure rate
Network scale	2-8 organizations	Commit latency, resource use
Record size	1 KB-10 MB metadata/payload	Storage overhead, upload/retrieval time
Consent policy	Role/resource/time combinations	Authorization accuracy, decision time
Attack simulation	Unauthorized/tampered requests	Detection rate, false acceptance rate
Node failure	Peer/orderer availability	Recovery time, transaction continuity

Performance should be measured using transaction latency, throughput, CPU utilization, memory utilization, ledger growth, and query response time. Latency should be reported as mean, median, and high percentile values rather than only a single average. Throughput should be measured in committed transactions per second under controlled workloads. Security experiments should report true positives, false positives, false negatives, and true negatives for authorization and attack detection where applicable.

A useful baseline is a conventional centralized EHR access service using a relational database and application-level access control. The comparison should not imply that blockchain is inherently more secure; instead, it should evaluate which security and accountability properties are obtained and what performance overhead is introduced. The comparison should include a centralized database, a blockchain-only design, and the proposed hybrid Fabric architecture where feasible.

9. Analytical Results and Discussion:

Because this manuscript presents a framework rather than a report of a completed clinical deployment, numerical performance values should be inserted only after the described experiments are executed. This distinction is essential for publication integrity. The expected analytical behavior, however, can be stated from the architecture. Increasing transaction concurrency is expected to increase latency after the network approaches its processing capacity. Increasing the number of endorsing organizations is also expected to increase coordination overhead. Conversely, moving large clinical objects off-chain should prevent ledger growth from being proportional to the full file size.

The most important expected security benefit is auditability. In a centralized system, a privileged database administrator may be able to alter records or logs without leaving an independently verifiable history. In HF-Secure Health, record creation, consent changes, access requests, and revocations become ledger transactions endorsed according to consortium policy. This does not eliminate insider threats, but it raises the cost of undetected manipulation and creates evidence for forensic review.

The hybrid storage model is expected to provide a practical balance between integrity and scalability. Storing a hash and metadata on-chain is significantly smaller than storing a medical image or complete clinical document. At retrieval time, the hash comparison provides an independent integrity check. The principal trade-off is that availability now depends on the external storage system. Consequently, redundant storage, backups, access logging, and disaster recovery must be part of the deployment architecture.

Patient consent is another major advantage of the proposed design. Conventional role-based access control can determine whether a doctor has a clinical role, but it does not necessarily establish whether that doctor should access a specific patient's record for a specific purpose during a specific period. The proposed policy combines role, organization, resource type, purpose, consent, and time. This creates a more precise authorization model. However, it also increases policy-management complexity and requires carefully designed user interfaces.

Interoperability is supported by using FHIR-aligned metadata rather than inventing a proprietary blockchain data model. This can reduce integration friction with existing healthcare applications. Nevertheless, semantic interoperability remains a socio-technical problem involving terminology mappings, data quality, identity matching, and organizational governance. Blockchain can provide trusted provenance but cannot automatically resolve inconsistent clinical semantics.

A key design insight is that Hyperledger Fabric should be used selectively. Not every healthcare interaction requires a blockchain transaction. High-frequency sensor streams, large images, and continuously changing data are better managed by specialized databases or object stores. The ledger should record events that require shared trust, provenance, consent, integrity verification, or multi-party accountability. This selective approach is likely to be more scalable than treating the blockchain as a universal database.

10. Limitations:

The proposed framework has several limitations. First, a Fabric network does not automatically guarantee clinical correctness. Incorrect data entered by an authorized provider can still be committed. Blockchain establishes provenance and integrity of recorded events, not truthfulness of the underlying clinical observation. Second, patient identity recovery, certificate revocation, and lost credentials require operational procedures beyond chaincode.

Third, off-chain storage creates a dependency on availability and key management. Encryption keys must be protected through an appropriate key-management service, and backup policies must be tested. Fourth, interoperability with legacy EHR systems can require substantial engineering because healthcare organizations use heterogeneous data formats and workflows. Fifth, a consortium must define governance rules covering on boarding, endorsement policies, dispute handling, node operation, incident response, and data retention.

Finally, the framework is not a substitute for regulatory or ethical review. Healthcare data are sensitive, and legal requirements differ by jurisdiction. A publication should therefore avoid broad statements such as 'fully compliant' unless a formal compliance assessment has been completed.

11. Future Enhancement:

Future research can extend HF-Secure Health in several directions. A first direction is decentralized identity and verifiable credentials for cross-institution authentication. A second is zero-knowledge proof mechanisms that allow a requester to prove possession of an authorization attribute without disclosing unnecessary identity information. A third is integration with IoMT devices, where only summarized events or integrity anchors are written to Fabric while raw sensor streams remain in edge/cloud storage.

A fourth direction is privacy-preserving analytics. Federated learning, secure multi-party computation, or differential privacy could allow research organizations to derive population-level knowledge without directly obtaining patient records. A fifth direction is cross-network interoperability between separate Fabric consortia. Finally, adaptive policy engines could use risk scores to strengthen authentication when access behavior deviates from normal patterns, while preserving deterministic authorization at the ledger level.

12. Conclusion:

This paper proposed HF-Secure Health, a Hyperledger Fabric-based permissioned framework for secure and privacy-preserving healthcare data management. The architecture uses the blockchain as a shared trust, provenance, consent, and audit layer while keeping large clinical payloads encrypted in controlled off-chain storage. Fabric identities, organizational governance, endorsement policies, and chaincode-based authorization provide a foundation for multi-party healthcare collaboration. FHIR-aligned metadata improve interoperability, while cryptographic hashes allow the integrity of externally stored records to be verified.

The framework is designed around a practical principle: healthcare blockchain should not attempt to place every medical datum on-chain. Instead, blockchain should protect the events and relationships for which shared trust is valuable. The proposed combination of consent lifecycle management, fine-grained authorization, hybrid storage, provenance, and standardized metadata addresses limitations found in many earlier designs. The next step is a reproducible Hyperledger Fabric implementation followed by controlled benchmarking against centralized and alternative blockchain architectures. Such evaluation will allow numerical claims about throughput, latency, storage, resilience, and security to be supported by measured evidence.

References:

1. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *Journal of Medical Systems*, 40, 218. <https://doi.org/10.1007/s10916-016-0574-6>
2. Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information*, 8(2), 44. <https://doi.org/10.3390/info8020044>
3. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational and Structural Biotechnology Journal*, 16, 267-278. <https://doi.org/10.1016/j.csbj.2018.07.004>
4. Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient Healthcare Data Sharing via Blockchain. *Applied Sciences*, 9(6), 1207. <https://doi.org/10.3390/app9061207>
5. Guo, H., Li, W., Nejad, M., & Shen, C.-C. (2019). Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture. *arXiv/IEEE-related preprint*. <https://doi.org/10.48550/arXiv.1906.01188>
6. Mayer, A. H., da Costa, C. A., & Righi, R. R. (2020). Electronic health records in a Blockchain: A systematic review. *Health Informatics Journal*, 26(1). <https://doi.org/10.1177/1460458219866350>
7. Wu, G., Wang, S., Ning, Z., & Zhu, B. (2022). Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. *IEEE Journal of Biomedical and Health Informatics*, 26(5), 1917-1927. <https://doi.org/10.1109/JBHI.2021.3123643>

8. Uddin, M., Memon, M. S., Memon, I., Ali, I., Memon, J., Abdelhaq, M., et al. (2021). Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. *Computers, Materials & Continua*, 68(2), 2377-2397. <https://doi.org/10.32604/cmc.2021.015354>
9. Ndzimakhwe, M., Telukdarie, A., Munien, I., Vermeulen, A., Chude-Okonkwo, U. K., & Philbin, S. P. (2023). A Framework for User-Focused Electronic Health Record System Leveraging Hyperledger Fabric. *Information*, 14(1), 51. <https://doi.org/10.3390/info14010051>
10. Hasnain, M., Albogamy, F. R., Alamri, S. S., Ghani, I., & Mehboob, B. (2023). The Hyperledger fabric as a Blockchain framework preserves the security of electronic health records. *Frontiers in Public Health*, 11, 1272787. <https://doi.org/10.3389/fpubh.2023.1272787>