IJVAST | Vol. 2, Issue 3 | July 2026 | Open Access — Peer Reviewed Research Paper

# Blockchain-Based Secure Health Records Sharing Framework

Diraj Kulkarni[1], Amol Navale[2]
*Department of Computer Engineering*
*COEP Technological University, Pune, Maharashtra, India*

***Abstract*—**Electronic Health Records (EHRs) are increasingly shared across hospitals, diagnostic centers, insurers, and patients, yet conventional centralized storage architectures remain vulnerable to single points of failure, unauthorized access, and lack of patient-controlled consent. This paper proposes a blockchain-based framework for secure and auditable sharing of health records that combines a permissioned blockchain for access-control and audit-trail management with off-chain encrypted storage for the bulk medical data itself. Smart contracts enforce patient-defined consent policies, granting and revoking provider access without intermediary involvement, while cryptographic hashes anchored on-chain guarantee record integrity and tamper-evidence. A prototype was implemented using Hyperledger Fabric for the permissioned ledger and IPFS for encrypted off-chain storage, and evaluated for transaction throughput, access-grant latency, and storage overhead against a traditional centralized EHR system. Results show that the proposed framework achieves strong data integrity and fine-grained consent enforcement with acceptable latency overhead, and that off-chain storage keeps on-chain footprint minimal even as record volume scales. The framework demonstrates that blockchain-based access control can meaningfully improve patient autonomy, auditability, and interoperability in multi-institutional healthcare data sharing without compromising performance for typical clinical workflows.

***Index Terms*—*Blockchain, Electronic Health Records, Smart Contracts, Hyperledger Fabric, Data Privacy, Access Control, Interoperability, Off-Chain Storage, IPFS, Healthcare Security.***

## I. INTRODUCTION

The digitization of healthcare has led to widespread adoption of Electronic Health Records (EHRs), enabling faster diagnosis, care coordination, and data-driven treatment decisions. However, EHR systems are typically built on centralized architectures managed by individual hospitals or health information exchanges, creating single points of failure, limiting patient control over their own data, and complicating secure sharing across institutional boundaries.

Patients frequently need their records accessible to multiple providers, insurers, and specialists, yet existing systems offer little transparency into who has accessed a record, when, and for what purpose. Data breaches involving centralized health databases have repeatedly exposed sensitive patient information, underscoring the need for architectures that minimize single points of trust and give patients direct control over consent.

Blockchain technology, with its properties of decentralization, immutability, and programmable smart contracts, offers a promising foundation for rebuilding health-record sharing around patient-centric access control and verifiable audit trails. This paper proposes and evaluates a blockchain-based framework in which a permissioned ledger manages access-control policies and audit logs, while

### *C. Off-Chain Storage and Interoperability*

Distributed storage systems such as IPFS have been combined with blockchain to store encrypted medical files off-chain, with only content hashes recorded on-chain, balancing data availability, storage cost, and immutability guarantees. Interoperability standards such as HL7 FHIR have also been proposed for structuring the underlying health-record data exchanged through such frameworks.

## III. PROPOSED FRAMEWORK

### *A. System Architecture*

The proposed framework consists of three layers: (1) a permissioned blockchain layer built on Hyperledger Fabric that manages identity, access-control policies, and audit logs; (2) an off-chain encrypted storage layer built on IPFS that stores the actual medical records; and (3) a client application layer through which patients, providers, and administrators interact with the system.

### *B. Identity and Access Management*

Each participant (patient, hospital, physician, insurer) is issued a unique digital identity via the Fabric Certificate Authority. Access to a given patient's records requires an explicit, on-chain consent grant recorded through a smart contract transaction, which can be time-bound or scope-limited to specific record categories.

 

encrypted medical data itself is stored off-chain to avoid the scalability and privacy limitations of storing raw health data on a blockchain.

## II. LITERATURE REVIEW

### *A. Blockchain in Healthcare*

Prior work has explored blockchain for healthcare applications including drug supply-chain tracking, clinical-trial data integrity, and health-insurance claim processing. Several studies have proposed blockchain-based EHR sharing architectures, generally converging on the pattern of storing only metadata, hashes, and access-control logic on-chain while keeping bulk medical data off-chain for scalability and privacy.

### *B. Access Control and Consent Management*

Smart-contract-based consent management has been proposed as a mechanism for patients to grant, restrict, and revoke provider access dynamically, replacing static institutional data-sharing agreements. Role-based and attribute-based access-control models implemented via smart contracts allow fine-grained, auditable permission enforcement.

### *C. Smart Contract Design*

Chaincode (smart contracts) implement three core functions: granting access, revoking access, and logging every access event as an immutable transaction. When a provider requests a record, the chaincode verifies an active consent grant before returning the decryption key reference and the IPFS content hash.

### *D. Data Encryption and Storage*

Medical records are encrypted client-side using AES-256 before being uploaded to IPFS. The resulting content hash and a reference to the encryption key (itself protected via patient-controlled key management) are recorded on-chain, ensuring that raw patient data never resides directly on the blockchain.

The physical and functional comparison between the proposed framework and a traditional centralized EHR architecture is summarized in Table I.

**TABLE I — Comparison of Proposed Framework and Traditional Centralized EHR Architecture**

| Feature | Traditional Centralized EHR | Proposed Blockchain Framework |
|---|---|---|
| Single point of failure | Yes | No |
| Patient-controlled consent | Limited | Fine-grained, revocable |
| Audit trail immutability | Modifiable logs | Immutable, on-chain |
| Data storage location | Centralized database | Off-chain (encrypted) + on-chain hash |
| Cross-institution interoperability | Low | High (shared ledger) |

## IV. IMPLEMENTATION

A prototype was implemented using Hyperledger Fabric v2.5 for the permissioned blockchain network, comprising four organizations representing a hospital, a diagnostic laboratory, an insurance provider, and a certificate authority, each operating a peer node. Chaincode was developed in Go and deployed across the network using Fabric's standard endorsement and ordering services.

IPFS was used for off-chain encrypted file storage, with a private IPFS cluster deployed to avoid public exposure of encrypted health data. A React-based web client allowed patients to view, grant, and revoke access, while a REST API gateway mediated interactions between the client application and the Fabric network using the Fabric SDK.

## V. EVALUATION METHODOLOGY

### *A. Test Environment*

The prototype network was deployed across four virtual nodes with 4 vCPUs and 8 GB RAM each, connected over a simulated local network to emulate a multi-institutional deployment.

### *B. Performance Metrics*

Transaction throughput (transactions per second), access-grant latency, record-retrieval latency, and on-chain storage overhead were measured using Hyperledger Caliper across varying transaction loads and record volumes.

### *C. Security Evaluation*

The framework's resistance to unauthorized access, replay attacks, and tampering was evaluated through simulated adversarial scenarios, including attempts to

access records without valid consent grants and attempts to modify off-chain data without invalidating the on-chain hash.

**TABLE II — Transaction Throughput Under Varying Concurrent Client Load**

| Concurrent Clients | Avg. Throughput (TPS) | Avg. Access-Grant Latency (s) |
|---|---|---|
| 25 | 162 | 1.2 |
| 50 | 156 | 1.5 |
| 100 | 148 | 1.8 |
| 150 | 131 | 2.4 |
| 200 | 119 | 3.1 |

## VI. RESULTS AND DISCUSSION

### *A. Transaction Throughput*

The permissioned network sustained an average throughput of 148 transactions per second for access-grant and revocation operations under a load of 100 concurrent clients, with throughput results across varying loads summarized in Table II.

### *B. Access-Grant and Retrieval Latency*

Average access-grant latency was 1.8 seconds and average record-retrieval latency (including off-chain IPFS fetch and client-side decryption) was 2.4 seconds, both within acceptable bounds for typical clinical workflows that are not real-time critical.

### *C. Storage Overhead*

On-chain storage overhead remained minimal, at approximately 0.6 KB per record for the hash, metadata, and access-log entry, regardless of the underlying medical file size, confirming that off-chain storage effectively decouples blockchain scalability from health-record data volume.

### *D. Security Evaluation Results*

All simulated unauthorized-access attempts were correctly rejected by the chaincode's consent-verification logic, and all off-chain tampering attempts were detected through hash mismatch upon retrieval, confirming the framework's tamper-evidence and access-control guarantees.

## VII. COMPARATIVE ANALYSIS

Table III compares the proposed framework against a traditional centralized EHR system across key dimensions including single point of failure risk, patient consent control, audit transparency, and data-breach exposure. The blockchain-based framework eliminates single points of failure for access-control decisions, provides patient-controlled, revocable consent, and generates an immutable audit trail, at the cost of modest additional latency compared to direct centralized database access.

## VIII. CHALLENGES AND LIMITATIONS

Key limitations include the operational complexity of managing a multi-institutional permissioned network, the need for standardized onboarding and key-management procedures across participating organizations, and residual reliance on off-chain storage availability. Regulatory alignment with healthcare data-protection frameworks such as HIPAA and India's Digital Personal Data Protection Act also requires careful mapping of on-chain audit data to compliance requirements.

**TABLE III — Comparative Analysis Across Key System Dimensions**

| Dimension | Centralized EHR | Blockchain Framework |
|---|---|---|
| Breach exposure | High (single target) | Low (distributed, encrypted) |
| Consent revocation | Manual, slow | Real-time, on-chain |
| Audit transparency | Limited | Full, immutable |
| Access latency | Low (~0.3s) | Moderate (~1.8-2.4s) |
| Deployment complexity | Low | Moderate-High |

## IX. FUTURE SCOPE

Future work includes integrating HL7 FHIR-compliant data models to improve interoperability with existing hospital information systems, exploring zero-knowledge proof mechanisms for privacy-preserving verification of record attributes without revealing underlying data, and extending the framework to support cross-chain interoperability between independently governed regional health-information networks. Incorporating attribute-based encryption for more granular, policy-driven access control is also a promising direction.

## X. CONCLUSION

This paper presented a blockchain-based framework for secure health-record sharing that combines a permissioned Hyperledger Fabric ledger for access control and audit logging with off-chain encrypted storage on IPFS for the underlying medical data. Evaluation of a working prototype demonstrated acceptable transaction throughput, access-grant latency, and minimal on-chain storage overhead, while security testing confirmed robust enforcement of patient consent and tamper-evidence of stored records. The results indicate that blockchain-based architectures can meaningfully strengthen patient autonomy, auditability, and trust in multi-institutional health-record sharing, and future integration with interoperability standards and privacy-preserving cryptographic techniques can further improve real-world deployability.

## XI. REFERENCES

[1] Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In Proc. Int. Conf. Open and Big Data, 25-30.

[2] Xia, Q., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., and Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757-14767.

[3] Dagher, G.G., Mohler, J., Milojkovic, M., and Marella, P.B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283-297.

[4] Zhang, P., White, J., Schmidt, D.C., Lenz, G., and Rosenbloom, S.T. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. Computational and Structural Biotechnology Journal, 16, 267-278.

[5] Roehrs, A., da Costa, C.A., and da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. Journal of Biomedical Informatics, 71, 70-81.

[6] Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 218.

[7] Androulaki, E., Barger, A., Bortnikov, V., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In Proc. EuroSys, 1-15.

[8] Benet, J. (2014). IPFS — Content addressed, versioned, P2P file system. arXiv:1407.3561.

[9] Kuo, T.T., Kim, H.E., and Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.

[10] Rifi, N., Rachkidi, E., Agoulmine, N., and Taher, N.C. (2017). Towards using blockchain technology for eHealth data access management. In Proc. IEEE Int. Conf. Advances in Biomedical Engineering, 1-4.

[11] Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., and Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of Medical Systems, 42(7), 130.

[12] Liang, X., Zhao, J., Shetty, S., Liu, J., and Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proc. IEEE PIMRC, 1-5.

[13] Ekblaw, A., Azaria, A., Halamka, J.D., and Lippman, A. (2016). A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data. In Proc. IEEE Open and Big Data Conf., 13.

[14] HL7 International. (2019). HL7 FHIR Release 4 — Fast Healthcare Interoperability Resources specification.

[15] Chen, Y., Ding, S., Xu, Z., Zheng, H., and Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. Journal of Medical Systems, 43(1), 5.

[16] Vora, J., Nayyar, A., Tanwar, S., et al. (2018). BHEEM: A blockchain-based framework for securing electronic health records. In Proc. IEEE Globecom Workshops, 1-6.

[17] Shahnaz, A., Qamar, U., and Khalid, A. (2019). Using blockchain for electronic health records. IEEE Access, 7, 147782-147795.

[18] Government of India. (2023). Digital Personal Data Protection Act, 2023.

[19] U.S. Department of Health and Human Services. (1996). Health Insurance Portability and Accountability Act (HIPAA).

[20] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available: bitcoin.org.


ISSN: Applied For (2026) | DOI: 10.XXXXX/IJVAST.2026.XXXXX | Open Access — CC BY 4.0 License