



# Blockchain-Based Secure Electronic Health Record Sharing: A Privacy-Preserving Framework for Interoperable Healthcare Systems

**Dr. Neha Mehta<sup>1</sup>**

Research Scholar<sup>1</sup>

Department of Computer Science and Engineering  
National Institute of Technology, Jaipur, Rajasthan, India  
neha.mehta@nitjindia.in

## Abstract

The rapid digitization of healthcare has resulted in the widespread adoption of Electronic Health Records (EHRs), electronic prescriptions, laboratory systems, medical imaging platforms, and other digital health services. Although these technologies improve the availability and efficiency of medical information, healthcare organizations frequently operate heterogeneous systems that make secure and seamless information exchange difficult. Patient information may be distributed across hospitals, diagnostic laboratories, clinics, pharmacies, insurance providers, and specialist centers. Conventional centralized architectures can create challenges related to interoperability, privacy, access control, data ownership, auditability, and single points of failure. Blockchain technology has emerged as a potential mechanism for improving trust and traceability in healthcare information exchange because it provides distributed transaction recording, cryptographic verification, and tamper-evident audit trails.

This paper investigates the use of blockchain technology for secure electronic health record sharing and proposes a conceptual privacy-preserving framework for interoperable healthcare systems. The proposed framework separates sensitive medical data from blockchain transactions and uses blockchain primarily for access-control records, integrity verification, consent management, and auditable event tracking. A hybrid architecture combining off-chain medical-data storage, cryptographic hashes, smart contracts, decentralized identity, and patient-controlled consent is presented. The study analyzes how blockchain can address important healthcare challenges, including unauthorized access, fragmented records, lack of transparency, and difficulties in maintaining reliable audit trails. It also examines the limitations of blockchain, including scalability, storage requirements, key management, privacy leakage, interoperability, smart-contract vulnerabilities, and regulatory considerations.

The paper proposes a role-based and consent-aware access mechanism in which patients can authorize healthcare providers to access selected categories of information for predefined periods. A conceptual risk model is also introduced to evaluate access requests according to identity, purpose, data sensitivity, and authorization status. The paper concludes that blockchain should not be considered a replacement for existing healthcare databases but rather as a complementary trust and coordination layer. Future research should focus on interoperable standards, privacy-preserving cryptography, decentralized identity, efficient consensus mechanisms, cross-institutional testing, and integration with emerging healthcare technologies.

**Keywords:** Blockchain, Electronic Health Records, Healthcare Data Security, Privacy, Interoperability, Smart Contracts, Consent Management, Medical Data, Decentralized Identity, Healthcare Information Systems

## 1. Introduction

Healthcare organizations increasingly depend on digital information systems to manage patient information. Electronic Health Records have replaced many traditional paper-based records and enable healthcare professionals to store and retrieve clinical information electronically.

An EHR may contain:

- Patient demographics
- Medical history
- Diagnoses
- Laboratory results
- Prescriptions
- Medical images
- Clinical notes
- Allergies
- Treatment information
- Discharge summaries

The availability of these records can significantly improve healthcare delivery.

However, healthcare information is frequently distributed among different organizations.

A patient may receive treatment from:



HospitalA→LaboratoryB→SpecialistC→PharmacyD  
Hospital\_A \rightarrow Laboratory\_B \rightarrow Specialist\_C \rightarrow Pharmacy\_D

Each organization may use different software, databases, authentication mechanisms, and data formats.

This creates an interoperability problem.

## 1.1 Healthcare Data Interoperability

Interoperability refers to the ability of different systems to exchange and use information.

A simplified model is:

SystemA→Data→SystemB  
System\_A \rightarrow Data \rightarrow System\_B

However, successful interoperability requires more than simply transmitting data.

The receiving system must be able to determine:

1. Who generated the information?
2. Whether the information has been modified.
3. Who is authorized to access it?
4. Why the information is being accessed?
5. When the access occurred?
6. Whether the patient provided appropriate consent?

These requirements create a strong need for reliable authentication, authorization, integrity verification, and auditing.

## 1.2 Motivation

Centralized healthcare information systems can provide efficient data management, but they also introduce concentration of trust.

If:

Database → Central Authority Database → Central Authority

then the central authority generally controls:

- Data storage
- Access
- Modification
- Logging
- Availability

A compromise of the central infrastructure can potentially affect a large quantity of information.

Blockchain introduces a distributed ledger model in which transactions can be recorded across participating entities.

A simplified blockchain transaction is:

$$T_i = \text{Hash}(\text{Data}_i) + \text{Metadata}_i \quad T_i = \text{Hash}(\text{Data}_i) + \text{Metadata}_i$$

The resulting record can be verified later to determine whether associated information has changed.

## 1.3 Problem Statement

The central problem addressed by this paper is:

**How can blockchain technology be integrated with electronic health record systems to improve security, patient-controlled consent, auditability, and interoperability while preserving privacy and maintaining practical system performance?**

## 1.4 Research Objectives

The objectives of this study are:

1. To examine security challenges associated with EHR sharing.
2. To analyze blockchain technology in the healthcare context.
3. To investigate blockchain-based access-control mechanisms.
4. To develop a privacy-preserving EHR sharing architecture.

5. To examine the role of smart contracts in consent management.
6. To analyze interoperability challenges.
7. To identify scalability and privacy limitations.
8. To propose a conceptual security and risk model.
9. To identify future research directions.

## 1.5 Contributions

The major contributions of this paper are:

- A conceptual blockchain architecture for EHR sharing.
- A hybrid on-chain/off-chain storage model.
- A patient-oriented consent-management mechanism.
- A role- and purpose-aware access-control model.
- A blockchain-based audit mechanism.
- Analysis of privacy, scalability, interoperability, and key-management challenges.
- Identification of future research opportunities.

## 2. Electronic Health Record Systems

An Electronic Health Record is a digital representation of patient-related healthcare information.

### 2.1 Components of EHR Data

EHR information can be divided into several categories.

#### Administrative Data

Examples include:

- Patient identification
- Contact information
- Insurance information



## Clinical Data

Examples include:

- Diagnoses
- Symptoms
- Medical history
- Treatment records

## Diagnostic Data

Examples include:

- Blood-test results
- Imaging results
- Pathology reports

## Medication Data

Examples include:

- Prescriptions
- Medication history
- Dosage information

## Clinical Documentation

Examples include:

- Physician notes
- Nursing notes
- Discharge summaries

The sensitivity of this information requires strong protection.

## 3. Challenges in EHR Sharing

### 3.1 Fragmented Storage

Patient information may be stored across multiple institutions.

This can result in:

$PatientData = \{D_1, D_2, D_3, \dots, D_n\}$   $PatientData = \{D_1, D_2, D_3, \dots, D_n\}$

where each  $D_i$  may belong to a different organization.

### 3.2 Unauthorized Access

Healthcare information can be accessed by individuals who do not have an appropriate clinical or administrative purpose.

### 3.3 Data Tampering

Medical information must remain accurate.

If:

$D_{original} \neq D_{current}$   $D_{original} \neq D_{current}$

the system should be able to detect unauthorized modification.

### 3.4 Limited Patient Control

Traditional healthcare systems may not provide patients with sufficiently transparent mechanisms for managing access to their information.

### 3.5 Auditability

Organizations need to determine:

- Who accessed the data?
- What data were accessed?
- When were they accessed?
- What was the purpose?
- Was access authorized?

### 3.6 Interoperability

Different institutions may use different:

- Data structures
- APIs
- Terminologies
- Identity systems
- Security architectures

This complicates information exchange.

## 4. Blockchain Technology

Blockchain is a distributed ledger technology that records transactions in a sequence of linked blocks.

A simplified block can be represented as:

$$B_i = \text{Hash}(B_{i-1} + \text{Transactions}_i + \text{Timestamp}_i)$$

The connection between blocks creates a chain.

## 4.1 Distributed Ledger

Instead of relying on one database:

Database → Single Organization Database \rightarrow Single \ Organization

a distributed ledger can be maintained by multiple authorized participants.

## 4.2 Cryptographic Hashing

A hash function converts information into a fixed-length representation.

$h = H(D)$

If the underlying data changes:

$D' \neq D$

then, with overwhelming probability:

$H(D') \neq H(D)$

This makes hashes useful for integrity verification.

## 4.3 Consensus

Blockchain participants need mechanisms for agreeing on valid transactions.

In healthcare applications, permissioned blockchain architectures may be more appropriate than completely public networks because participating organizations are generally identifiable.

## 4.4 Smart Contracts

A smart contract is programmable logic executed according to predefined conditions.



Conceptually:

IF Authorization=TrueIF\;Authorization=True THEN GrantAccessTHEN\;GrantAccess

Smart contracts can support consent and authorization processes.

## 5. Blockchain in Healthcare

Blockchain has been investigated for several healthcare applications.

These include:

- EHR sharing
- Medical supply chains
- Clinical research
- Drug traceability
- Insurance claims
- Patient identity
- Consent management
- Medical-device data

The technology is particularly relevant where multiple organizations need to coordinate while maintaining an auditable record.

## 6. Proposed Blockchain-Based EHR Architecture

The proposed system contains seven major components.

### 1. Patient

The patient owns or controls consent decisions.

### 2. Healthcare Provider

Hospitals and clinics request authorized access.



### 3. Diagnostic Provider

Laboratories and imaging centers contribute clinical information.

### 4. Blockchain Network

Authorized participants maintain the transaction ledger.

### 5. Smart Contract Layer

Automates consent and access-control policies.

### 6. Off-Chain Storage

Stores actual medical documents and large files.

### 7. Identity Service

Authenticates patients and healthcare professionals.

The architecture can be represented as:

Patient ↔ Identity ↔ SmartContract ↔ Blockchain  
Patient \leftrightharpoonup Identity \leftrightharpoonup SmartContract \leftrightharpoonup Blockchain

while:

MedicalData → OffChainStorage  
MedicalData \rightarrow OffChainStorage

The blockchain stores references, integrity information, permissions, and audit events rather than complete medical records.

## 7. On-Chain and Off-Chain Storage

Storing complete medical records directly on a blockchain may create substantial scalability and privacy concerns.

Therefore, this paper proposes a hybrid model.

### 7.1 Off-Chain Medical Data

Large files such as:

- MRI images
- CT scans
- X-rays
- Laboratory documents

can be stored in secure external storage.

### 7.2 Blockchain Metadata

The blockchain can contain:

- Record identifier
- Data hash
- Storage reference
- Timestamp
- Owner identifier
- Access policy
- Consent status

For a record DD:

$HD = \text{Hash}(D) \quad H\_D = \text{Hash}(D)$

When a user retrieves the record:

$H_{Retrieved} = Hash(D_{Retrieved})$   
 $H_{\{Retrieved\}} = Hash(D_{\{Retrieved\}})$

Integrity is verified when:

$H_{Retrieved} = HDH_{\{Retrieved\}} = H\_D$

## 8. Patient-Centric Consent Management

Consent is an important component of healthcare information sharing.

A patient may authorize:

Hospital A can access laboratory reports for 30 days.

The corresponding policy can be represented as:

$C = (Patient, Provider, DataType, Purpose, Duration)$   
 $C = (Patient, Provider, DataType, Purpose, Duration)$

For example:

$C = (P1, H1, LabData, Treatment, 30Days)$   
 $C = (P\_1, H\_1, LabData, Treatment, 30Days)$

### 8.1 Consent Grant

A patient submits a consent transaction.

$Grant(P, H, D, T)$   
 $Grant(P, H, D, T)$

where:

- PP = patient
- HH = healthcare provider
- DD = data category
- TT = validity period

## 8.2 Consent Revocation

The patient can revoke access:

$\text{Revoke}(P, H, D)$

Future requests are then rejected according to the updated policy.

## 8.3 Temporary Access

Temporary authorization can reduce unnecessary long-term access.

$\text{AccessTime} \leq \text{ExpiryTime}$

Once the permission expires:

$\text{Access} = \text{False}$

# 9. Role-Based Access Control

Healthcare organizations contain different categories of users.

Examples include:

- Physician
- Nurse
- Laboratory technician
- Pharmacist
- Administrator
- Researcher

Each role should receive only the privileges necessary for its legitimate function.

A role-based model can be expressed as:

$\text{Permission} = f(\text{Role}, \text{DataType}, \text{Purpose})$

For example:

| Role             | Patient Summary | Laboratory Data | Prescription | Administrative Data |
|------------------|-----------------|-----------------|--------------|---------------------|
| Physician        | Yes             | Yes             | Yes          | Limited             |
| Nurse            | Yes             | Limited         | Limited      | No                  |
| Laboratory Staff | Limited         | Yes             | No           | No                  |
| Pharmacist       | Limited         | Limited         | Yes          | No                  |
| Administrator    | Limited         | No              | No           | Yes                 |
| Researcher       | De-identified   | De-identified   | Limited      | No                  |

The exact permissions should depend on organizational policies and applicable regulations.

## 10. Purpose-Based Access Control

Role alone may not be sufficient.

A physician treating a patient may require access to medical information, while the same person may not require access for unrelated purposes.

Therefore:

$\text{Access} = f(\text{Identity}, \text{Role}, \text{Purpose}, \text{Consent}, \text{DataSensitivity})$

A request is approved only when the required conditions are satisfied.

## 11. Smart Contract for Access Control

A conceptual smart contract may perform the following steps:

1. Verify requester identity.
2. Identify requester role.
3. Identify requested data.
4. Determine purpose.

5. Check patient consent.
6. Check expiration.
7. Record the access event.
8. Approve or reject access.

The decision can be represented as:

$$A = \begin{cases} 1, & \text{if } R \wedge C \wedge P \wedge T = 0 \\ 0, & \text{Otherwise} \end{cases}$$

where:

- II = valid identity
- RR = valid role
- CC = valid consent
- PP = legitimate purpose
- TT = valid time period

## 12. Data Integrity Verification

Blockchain can support integrity verification.

Suppose a healthcare provider uploads a medical report DD.

The system calculates:

$$H = \text{Hash}(D)$$

The hash is recorded on the blockchain.

Later, when the document is retrieved:

$$H' = \text{Hash}(D')$$

The system checks:

$$H' = H$$

If the values differ:

$H' \neq H$

the system reports a possible modification.

## 13. Audit Trail

Every access event can generate a blockchain transaction.

A transaction can contain:

$T = (User, Record, Action, Time, Purpose, Result)$

Examples include:

- Record viewed
- Record uploaded
- Consent granted
- Consent revoked
- Access denied
- Record updated

The resulting audit trail can improve accountability.

## 14. Privacy Protection

Although blockchain provides integrity and auditability, it should not automatically be assumed to provide complete privacy.

Healthcare information requires additional protection.

### 14.1 Avoiding Raw Medical Data on Blockchain

The proposed architecture avoids storing complete patient records directly on the blockchain.

Instead:

Blockchain→MetadataBlockchain\rightarrow Metadata OffChain→MedicalDataOffChain\rightarrow MedicalData

## 14.2 Encryption

Medical data should be encrypted before storage.

Conceptually:

$C = \text{Encrypt}_K(D)$

where:

- DD = medical data
- KK = encryption key
- CC = ciphertext

Only authorized users should obtain the appropriate decryption capability.

## 15. Cryptographic Key Management

Key management is one of the most important practical issues.

If a patient loses a private key:

Keylost→AccessproblemKey\_{lost}\rightarrow Access\_{problem}

Therefore, a practical healthcare system should include:

- Secure key storage
- Recovery mechanisms
- Key rotation
- Multi-factor authentication
- Revocation mechanisms

## 15.1 Key Rotation

Keys may periodically be replaced.

$K_1 \rightarrow K_2 \rightarrow K_3$   $K_1 \rightarrow K_2 \rightarrow K_3$

The transition should be managed without unnecessarily disrupting authorized healthcare access.

## 16. Decentralized Identity

A decentralized identity architecture can potentially reduce dependence on a single identity provider.

A user may possess a verifiable identity credential.

Conceptually:

Identity = Credential + Verification

A healthcare professional can prove:

- Professional identity
- Organizational affiliation
- Role
- Authorization

without necessarily exposing unrelated personal information.

## 17. Interoperability

Blockchain alone does not solve interoperability.

Different systems must still agree on:

- Data formats
- Terminologies

- APIs
- Identity formats
- Security protocols

An interoperability architecture can be represented as:

HospitalA ↔ InteroperabilityLayer ↔ HospitalB  
Hospital\_A \leftrightharpoon InteroperabilityLayer \leftrightharpoon Hospital\_B

The blockchain can provide trust and auditability around the exchange.

## 18. Proposed Secure Data-Sharing Workflow

The proposed workflow consists of the following steps.

### Step 1: Patient Registration

The patient receives a secure digital identity.

### Step 2: Record Creation

A healthcare organization creates an EHR record.

### Step 3: Encryption

The record is encrypted.

### Step 4: Off-Chain Storage

The encrypted record is stored securely.

### Step 5: Hash Generation

The system calculates:



$H = \text{Hash}(D)$

### Step 6: Blockchain Registration

The hash and metadata are recorded.

### Step 7: Access Request

A healthcare professional requests access.

### Step 8: Consent Verification

The system verifies patient authorization.

### Step 9: Smart Contract Execution

The policy is evaluated.

### Step 10: Data Access

Authorized users receive appropriate access.

### Step 11: Audit Recording

The event is recorded.

## 19. Security Risk Model

The system can calculate a conceptual access risk score.

Let:

- II = identity confidence
- RR = role confidence

- CC = consent confidence
- DD = data sensitivity
- PP = purpose validity

A risk score can be defined as:

$$\text{Risk} = w_1(1-I) + w_2(1-R) + w_3(1-C) + w_4D + w_5(1-P)$$

where:

$$\sum_{i=1}^5 w_i = 1$$

A high score can trigger additional authentication or manual review.

## 20. Threat Model

The proposed system should consider multiple attacker categories.

### 20.1 External Attacker

Attempts to compromise network services or credentials.

### 20.2 Malicious Insider

An authorized employee attempts to access information beyond legitimate requirements.

### 20.3 Compromised Account

An attacker obtains valid user credentials.

### 20.4 Malicious Data Provider

A participating organization provides incorrect or manipulated information.

## 20.5 Smart Contract Attacker

Attempts to exploit logic vulnerabilities.

## 20.6 Storage Attacker

Attempts to modify or delete off-chain records.

Blockchain integrity does not automatically protect external storage.

Therefore:

$\text{BlockchainSecurity} \neq \text{CompleteSystemSecurity}$

The entire architecture must be protected.

# 21. Blockchain Security Threats

## 21.1 Private-Key Compromise

If an attacker obtains a user's private key, unauthorized transactions may be created.

## 21.2 Smart Contract Vulnerabilities

Incorrect contract logic may result in unintended access.

## 21.3 Consensus Attacks

Distributed networks require protection against manipulation of consensus mechanisms.

## 21.4 Metadata Leakage

Even if medical data are not stored directly, transaction metadata may reveal information about healthcare activity.

## 21.5 Availability

Blockchain infrastructure must remain available when healthcare providers require information.

## 22. Scalability

Healthcare generates large quantities of data.

For NN patients:

$$\text{DataVolume} = N \times \text{AveragePatientData}$$

If the system stores large medical files directly on-chain, storage requirements can increase rapidly.

Therefore:

$$\text{OffChainStorage} + \text{OnChainVerification}$$

is generally more practical for large healthcare datasets.

## 23. Performance Considerations

Healthcare applications can require rapid access.

System response time can be represented as:

$$T_{\text{total}} = T_{\text{authentication}} + T_{\text{blockchain}} + T_{\text{storage}} + T_{\text{decryption}}$$
$$T_{\text{total}} = T_{\text{authentication}} + T_{\text{blockchain}} + T_{\text{storage}} + T_{\text{decryption}}$$

The architecture should minimize unnecessary blockchain operations.

For example, frequent large-data transfers should not require storing the complete file on the ledger.

## 24. Comparative Analysis

| Architecture            | Security       | Patient Control  | Auditability | Scalability    | Interoperability |
|-------------------------|----------------|------------------|--------------|----------------|------------------|
| Centralized EHR         | Moderate       | Limited          | Moderate     | High           | Moderate         |
| Distributed Database    | High           | Moderate         | Moderate     | High           | Moderate         |
| Public Blockchain       | High integrity | Potentially high | High         | Lower          | Variable         |
| Permissioned Blockchain | High           | High             | High         | Better         | High             |
| Proposed Hybrid Model   | High           | High             | High         | High potential | High potential   |

The comparison is conceptual rather than a measured experimental benchmark.

## 25. Advantages of the Proposed Framework

### 25.1 Improved Auditability

Blockchain provides a tamper-evident record of transactions.

### 25.2 Patient-Centered Consent

Patients can participate directly in access decisions.

### 25.3 Data Integrity

Hashes can be used to detect unauthorized modification.

## 25.4 Reduced Single Point of Trust

Multiple healthcare organizations can participate in a shared permissioned network.

## 25.5 Controlled Access

Smart contracts can automate authorization rules.

## 25.6 Hybrid Storage

Large medical files remain outside the blockchain.

# 26. Limitations

## 26.1 Key Management

Patients and healthcare professionals may find cryptographic key management difficult.

## 26.2 Scalability

Large healthcare networks may generate a substantial number of transactions.

## 26.3 Interoperability

Blockchain does not automatically make different EHR systems interoperable.

## 26.4 Privacy

Transaction metadata can potentially reveal sensitive information.

## 26.5 Smart Contract Risks

Incorrect contract implementation may create security vulnerabilities.

## 26.6 Governance

Participating healthcare organizations must agree on:

- Network membership
- Data policies
- Governance
- Dispute resolution
- Responsibility

# 27. Proposed Experimental Methodology

A future implementation can evaluate the framework using a controlled healthcare data-sharing environment.

## 27.1 Experimental Components

The prototype can contain:

- Permissioned blockchain network
- EHR database
- Encrypted object storage
- Identity service
- Smart contracts
- Web-based healthcare interface

## 27.2 Test Scenarios

The system can be tested under:

1. Authorized access.
2. Unauthorized access.
3. Expired consent.
4. Revoked consent.
5. Modified medical record.
6. Compromised credentials.
7. High transaction volume.
8. Multiple healthcare organizations.

## 27.3 Evaluation Metrics

Potential metrics include:

- Access latency
- Transaction throughput
- Storage consumption
- Authentication time
- Authorization time
- Detection rate
- False-positive rate
- Availability
- Encryption overhead

## 28. Privacy-Preserving Research Directions

Future systems can integrate advanced privacy mechanisms.

### 28.1 Zero-Knowledge Proofs

A zero-knowledge approach may allow a user to demonstrate possession of an authorized credential without exposing unnecessary information.

Conceptually:

Prove(Authorization)Prove(Authorization)

without revealing:

UnnecessaryIdentityDataUnnecessaryIdentityData

## 28.2 Attribute-Based Encryption

Access can depend on attributes.

For example:

Doctor^Hospital^TreatmentPurposeDoctor\land HospitalA\land TreatmentPurpose

can define an access policy.

## 28.3 Differential Privacy

When healthcare data are used for research or analytics, differential privacy can reduce information leakage.

# 29. Integration with Artificial Intelligence

Blockchain and AI can complement each other.

AI can analyze healthcare data:

AI(Data)→PredictionAI(Data)\rightarrow Prediction

Blockchain can provide:

Blockchain→Integrity+Audit+ConsentBlockchain\rightarrow Integrity+Audit+Consent

Together:

AI+Blockchain→Secure Intelligent HealthcareAI+Blockchain\rightarrow Secure\ Intelligent\ Healthcare

AI may support:

- Disease prediction
- Risk assessment
- Medical image analysis
- Personalized treatment

Blockchain may support:

- Data provenance
- Consent
- Integrity
- Access logging

## 30. Integration with Internet of Medical Things

Internet of Medical Things devices can generate continuous patient information.

Examples include:

- Wearable sensors
- Heart monitors
- Glucose monitors
- Smart medical devices

A conceptual architecture is:

IoMT → Gateway → SecureStorageIoMT → Gateway → SecureStorage

with blockchain recording:

DeviceID+Timestamp+DataHashDeviceID+Timestamp+DataHash

This can support data provenance.

## 31. Ethical Considerations

### 31.1 Patient Autonomy

Patients should have meaningful control over how their information is shared.

### 31.2 Transparency

Organizations should clearly explain data-access policies.

### 31.3 Accountability

Every access event should be attributable to an authenticated entity.

### 31.4 Data Minimization

Users should receive only the information necessary for the intended purpose.

### 31.5 Right to Control Information

Healthcare systems must reconcile blockchain immutability with applicable requirements concerning modification, correction, and deletion of personal information.

## 32. Regulatory Considerations

Healthcare systems must comply with applicable privacy, security, medical-record, and data-governance requirements.

A blockchain architecture should therefore be designed around regulatory requirements rather than assuming that technical immutability is always desirable.

A practical architecture should support:

- Controlled access
- Data correction mechanisms
- Auditability
- Consent management
- Data minimization
- Secure identity
- Organizational accountability

## 33. Future Directions

### 33.1 Cross-Hospital Blockchain Networks

Future research can investigate blockchain networks connecting hospitals, laboratories, pharmacies, and insurance providers.

### 33.2 Global Interoperability

Standardized protocols could enable cross-border healthcare information exchange.

### 33.3 AI-Assisted Access Control

AI could identify unusual access patterns.

For example:

$\text{Behavior}_{\text{normal}} \rightarrow \text{Model} \rightarrow \text{Behavior}_{\text{normal}}$

and:

$\text{Behavior}_{\text{new}} \neq \text{Behavior}_{\text{normal}} \rightarrow \text{Behavior}_{\text{new}} \neq \text{Behavior}_{\text{normal}}$

could generate a security alert.

### 33.4 Continuous Authorization

Instead of authorizing a user once, future systems may continuously evaluate:

$Authorization = f(User, Device, Location, Purpose, Time)$   
 $Authorization = f(User, Device, Location, Purpose, Time)$

### 33.5 Quantum-Resistant Cryptography

Future healthcare blockchain systems may need cryptographic mechanisms designed to remain secure against emerging computational capabilities.

### 33.6 Decentralized Patient Identity

Patient identities could become portable across healthcare organizations.

### 33.7 Privacy-Preserving Analytics

Organizations may collaboratively analyze healthcare information without directly sharing all raw patient data.

## 34. Discussion

The proposed architecture demonstrates that blockchain can potentially provide a useful trust layer for healthcare information exchange. However, the technology should not be viewed as a universal solution to healthcare data security.

One of the most important architectural decisions is separating medical data from blockchain records. Medical records can be extremely large and sensitive. Storing them directly on a distributed ledger can create unnecessary storage, privacy, and performance problems.

The hybrid architecture addresses this challenge by storing encrypted medical information externally while recording integrity metadata and access events on the blockchain.



This creates a separation:

$\text{DataStorage} \neq \text{TrustManagement}$

The off-chain infrastructure is responsible for efficient storage, while blockchain provides an additional mechanism for integrity verification, authorization coordination, and auditing.

Patient-controlled consent is another important component. Traditional systems may require patients to trust healthcare organizations to manage access correctly. A consent-aware architecture provides a more transparent mechanism through which patients can specify who may access selected information and under what conditions.

However, patient control should not become an excessive burden. Healthcare decisions can occur under urgent circumstances where immediate access to relevant information may be necessary. Therefore, future systems should investigate carefully governed emergency-access mechanisms.

Another significant challenge is interoperability. Blockchain cannot solve differences between EHR platforms by itself. Data standards, APIs, terminology systems, and identity frameworks remain necessary.

The architecture should therefore be understood as:

$\text{Interoperability} + \text{Blockchain} + \text{Security}$

rather than:

$\text{Blockchain} = \text{Interoperability}$

Governance is equally important. A permissioned healthcare blockchain requires agreement among participating organizations regarding who can join the network, how smart contracts are updated, how disputes are handled, and who is responsible when technical failures occur.

The technology therefore creates not only a technical problem but also an organizational one.

## 35. Conclusion

Electronic Health Records have become an essential component of modern healthcare, but secure information sharing remains a significant challenge. Healthcare organizations frequently operate heterogeneous information systems, creating difficulties in interoperability, patient consent, access control, data integrity, and auditability.

This paper examined the potential role of blockchain technology in addressing these challenges and proposed a hybrid privacy-preserving architecture for secure EHR sharing.

The proposed framework separates medical data from blockchain metadata. Sensitive and large healthcare files remain in encrypted off-chain storage, while blockchain records can maintain hashes, consent information, access policies, timestamps, and audit events.

Smart contracts can automate access-control decisions by evaluating identity, role, purpose, patient consent, and authorization duration. A risk model was also introduced to support additional security controls for suspicious requests.

The study demonstrates that blockchain can provide useful capabilities for healthcare information exchange, particularly in environments involving multiple organizations that need a shared trust and audit mechanism.

Nevertheless, significant challenges remain. These include scalability, key management, privacy leakage, smart-contract vulnerabilities, interoperability, governance, regulatory requirements, and integration with existing EHR infrastructure.

Blockchain should therefore be viewed as a complementary technology rather than a replacement for conventional healthcare databases.

Future research should investigate decentralized identity, privacy-preserving cryptography, AI-assisted access monitoring, federated healthcare analytics, cross-hospital blockchain networks, and efficient interoperability mechanisms.

A successful healthcare blockchain system should ultimately satisfy the following objective:

Secure Sharing=Privacy+Integrity+Availability+Interoperability+Accountability  
Secure\ Sharing=  
Privacy+Integrity+Availability+Interoperability+Accountability

When these requirements are considered together, blockchain has the potential to become an important component of secure and patient-centered digital healthcare infrastructure.

## References

1. Kuo, T. T., Kim, H. E., & 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.
2. 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.
3. Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems*, 42, 130.
4. 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.
5. Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019). Implementing blockchain for efficient health care: Systematic review. *Journal of Medical Internet Research*, 21(2), e12439.
6. McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, 135, 62–75.
7. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare*, 7(2), 56.
8. Stagnaro, C. (2017). *Practical Guide to Implementing Blockchain in Healthcare*. HIMSS.
9. Kuo, T. T., Rojas, K., & Ohno-Machado, L. (2019). Comparison of blockchain platforms: A systematic review and healthcare-oriented framework. *Journal of the American Medical Informatics Association*, 26(5), 462–478.
10. Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient healthcare data sharing via blockchain. *Applied Sciences*, 9(6), 1207.
11. Dagher, G. G., Mohler, J., Milojkovic, M., & 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.
12. Hussein, A. F., ArunKumar, N., Annamalai, S., Jaber, M. M., & Ramirez-Gonzalez, G. (2019). A medical records managing and securing blockchain-based system supported by a genetic algorithm and discrete wavelet transform. *Cognitive Systems Research*, 52, 1–13.



13. Zhuang, Y., Sheets, L. R., Chen, Y. W., Shae, Z. Y., Tsai, J. J. P., & Shyu, C. R. (2020). A patient-centric health information exchange framework using blockchain technology. *IEEE Journal of Biomedical and Health Informatics*, 24(8), 2169–2176.
14. Roehrs, A., da Costa, C. A., & da Rosa Righi, R. (2017). OmniPHR: A distributed model of a personal health record. *Journal of Biomedical Informatics*, 71, 70–81.
15. World Health Organization. (2021). *Ethics and Governance of Artificial Intelligence for Health*. World Health Organization.