

Transforming Medical Records into Tamper-Proof Evidence: Role of Blockchain in Legal Risk Management

Parneet Kaur¹ and Renu Mahajan²

¹Uils, Chandigarh University, Mohali, India

Email: adv.parneet@gmail.com

²Amity University, Noida, India

Email: adv.renumahajan786@gmail.com

Abstract— The healthcare sector has made great progress during the last 50 years, yet it continues to face its most serious challenge with frontiers access control and data integrity problems. The system protects patient data through its decentralized structure which establishes unbreakable security boundaries that permit access to authorized users while enabling both transparent access and traceable activities. The main goal is to strengthen access control systems by guaranteeing only the authorized can access sensitive medical data and enhance security and integrity of medical data using decentralized blockchain methods. The traditional healthcare systems required centralized databases because each patient record had to be managed and stored by one organization which resulted in data manipulation and unauthorized access and total system security failure to protect data security within the system. Growing concerns about the security and privacy of data create a need for innovative solutions absolutely with an effective architecture based on blockchain to guarantee that all medical data and its sources are true, safe and accessible only by authorized users.[1] The proposed decentralized approach of blockchain enhances access control and integrity of medical data by providing a secure and transparent platform for patient record management. Each patient's information is stored on a blockchain as an individual record which is unable to be changed without consensus of a network. Given that blockchain is an impregnable technology, any attempts at illicit alteration of the data can be tracked and foiled.

Key words— Blockchain, Healthcare, medical records, Healthcare industry, Transparency, Security, Data Integrity, Access Control, Tamper-Proof.

I. METHODOLOGY



Fig 1

The researcher used the following online data sources which include Google scholar, IEEE, PubMed, Science Direct etc.

II. INTRODUCTION

The legal risks are increasing fast in the health sector where regulation, malpractice suits and negligence claims are many. The medical records are probably the most significant kind of evidence regarding these disputes because medical records may be used to establish timelines, verify treatments, or lethargic the quality of care given. It is on these documents that courts, regulatory commissions and insurance companies rely heavily for objective judgment and accurate interpretation. However, questions often arise about the accuracy of medical records, especially when it has been manipulated, lost or tampered.[2] Any physical document or electronic document storage system are always under constant threats from unauthorized changes, document removal, unintentional document loss and data corruption which all lead to ruinous outcomes for medical workers and adverse effects on judicial decisions. The current digital healthcare system requires medical record security through protective measures which meet both operational requirements and compliance standards. The healthcare sector underwent a transformation through blockchain technology because its permanent data storage system and decentralized infrastructure together with its cryptographic protection system enable complete medical record security control. The blockchain functions as a permanent record system which documents every transaction with time stamps to create an unalterable proof of evidence that possesses high legal validity. Smart contracts establish protection through human-made complementary elements which reduce the possibility of intentional fraud and human mistakes. [3]

A. Medical Records and Legal Risk Management

Medical records function as vital resources which help healthcare professionals deliver medical care while safeguarding patient safety and maintaining treatment standards and monitoring patient development through their clinical work. Successful patient care delivery requires medical professionals to work together efficiently while they maintain their specialized expertise and use their medical knowledge during the decision-making process. Medical records serve as essential evidence which courts utilize to establish their judicial determinations. The interdependence between medical malpractice cases and medical negligence cases help establish treatment timelines which assess treatment history and verify medical diagnosis and check treatment standard compliance and resolve patient-doctor conflicts. The documents function as verification tools which extend their reach to both courts and authorities and insurance companies to determine damage assessment and liability determination.

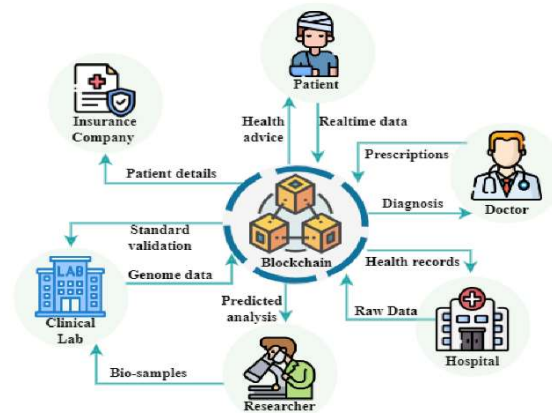


Fig 1: Role of Block chain in Health care

The two existing systems of paper and electronic medical records both contain defects which lead to persistent doubts about their ability to preserve accurate medical documentation. General risks include data breaches that risk compromising patient privacy and unauthorized users who can access sensitive information for purposes of data theft or data alteration and users who backdate entries to conceal their mistakes and users who create entirely fake records which they use to manipulate judicial outcomes. The court evidence becomes compromised through this process which results in evidence loss and patient trust loss in healthcare providers. [4]

The safety measures provide protection to some extent, but they lack complete security. The security of medical records remains at risk because hackers can execute advanced cyberattacks and because people with authorized access can make internal attacks and because organizations fail to maintain proper compliance monitoring. The evidence demonstrates that healthcare organizations require unbreakable security systems to protect medical data from unauthorized access in clinical and legal settings.

B. An Overview of Blockchain Technology

The security and record protection requirements of modern healthcare systems drive hospitals to adopt new technologies because traditional medical record systems suffer from security weaknesses and operational constraints. Blockchain technology functions as an innovative solution which enables development of systems which protect data through transparent and secure but unbreakable security methods.

The blockchain system uses distributed ledger technology to store data across multiple network nodes instead of relying on a centralized database system. The system's decentralized design reduced risks of data changes from unauthorized users while it removed all possibilities of single-point system failures. The primary advantage of blockchain technology exists because it creates permanent records which block any deletion of data that has been added to the blockchain system. [5] The Code of Professional Conduct requires attorneys to respect privileged communications with physicians, patients, and attorneys. The implementation of smart contracts which operate through blockchain-based contract execution will boost operational efficiency and legal accountability by enabling automatic verification of compliance requirements and management of patient consent and data sharing procedures.

Healthcare requirements can be talked about via various blockchain systems based upon its architectural designs. Public blockchains enable all users to access their network yet their transparency and audit capabilities fail to provide suitable protection for sensitive health information because HIPAA and India's Digital Personal Data Protection Act, 2023 create privacy constraints. Private blockchains, on the other hand, operate under the authority of one organization which establishes specific governance systems that permit the organization to perform rapid transactions while facing intense monitoring. The proposed solution would grant operational authority, but it would introduce the same centralization dangers that blockchains exist to prevent because users would gain complete power to alter information according to their preferences. Permissioned blockchains provide an alternative that allows access to approved parties, which secures role-based access while maintaining data confidentiality. The system will benefit healthcare organizations because it enables them to safeguard patient records while letting authorized individuals access the information. [6] Physicians, hospitals, insurers and regulators would have the liberty to access the correct information when needed.

The healthcare sector can implement blockchain technology to create secure electronic health records (EHRs) and trace medical supply chains for authenticating drug and medical device shipments while using blockchain to safeguard clinical trial data through unchangeable records and blockchain-based systems that control patient data exchange between medical facilities and different healthcare regions.

Healthcare providers can greatly reduce their legal risks which arise from data loss incidents and unauthorized access attempts and record tampering situations through the implementation of blockchain technology in their medical record systems. Blockchain technology stores medical records in a way that provides better evidence reliability for litigation cases because all alterations and record transactions are time-stamped and protected by cryptographic security and can be easily audited. The system strengthens evidence which supports malpractice claims while maintaining public trust and institutional confidence in blockchain technology use.[7]

II. BLOCKCHAIN BASED SOLUTIONS FOR TRANSFORMING MEDICAL RECORDS

Medical records stored as blockchain technology maintain permanent record security which enables their time-based authenticity verifiable through multiple traceable methods. The ecosystem depends on smart contracts to perform essential functions which include automatic processes for recording activities and obtaining consent and managing access permissions. A smart contract example demonstrates how a system creates locks to protect patient consent for documents which authorize doctor and insurer and law enforcement access while recording all access permissions through role-based or time-limited access methods into the blockchain system.

The blockchain enables healthcare organizations to share data between their hospitals and clinics and their insurance companies and regulatory bodies. The system enables health data to be shared across multiple healthcare organizations through its seamless interoperability feature. The system maintains an up-to-date record of all access points and data changes which decreases the risk of unauthorized data access and modifications. Medical records now function as official legal documents that courts must recognize because their chain-of-

custody establishes their authenticity which requires specialized custody procedures. The blockchain technology provides cryptographic proofs and time-stamping functions that healthcare organizations can use to establish data integrity when handling medical malpractice and negligence cases for legal risk management purposes.[8] Pilot schemes across the world substantially demonstrate that medical records can be saved on blockchain technology while taking away the legal concerns. The e-Health Foundation of Estonia, for example, implies that blockchain technology is incorporated into the national electronic health record (EHR) system to ensure data integrity and enable patients to control who has access to their medical records. MedRec, the project created by MIT USA, does the same but use blockchain technology in managing Electronic Health Record (EHR) of patients, through giving access to both patients and health care providers decentral and securely, with identifiable audit trails. Similarly collaborated Guard time, the blockchain-based cybersecurity company with European health institutions, to secure patient private data and ensure compliance with data protection protocols. Although at an infant stage, the blockchain application in the healthcare setting is garnering its stride in India. In the NITI Aayog-Phoenix pilot project with an emphasis on interoperability and patient consent management, the use of blockchain technology to create a tamper-proof digital health ecosystem was explored.[9] The Telangana government is working with partners to develop blockchain-based health data management systems to enhance transparency and protection of records. Other private sector initiatives such as Lifeserver and Medicalchain are testing blockchain-based health record platforms which may one day serve as verifiable evidence in cases of medical malpractice. The groundwork for this scalable adoption is established by such case studies, demonstrating that blockchain will enhance security, interoperability and transparency of medical records in the health care sector and increase their evidentiary value in court to address legal risks.

III. LEGAL AND REGULATORY FRAMEWORK

The legal and regulatory framework hugely influences the evidentiary value and requirement of blockchain-based health records. The Bharatiya Sakshya Adhiniyam of 2023, the new enactment mediating the admissibility of electronic evidence in India; has replaced the Indian Evidence Act, 1872. Electronic documents, as well as data stored on blockchain, will be admissible as evidence if they comply with the required conditions of integrity, authenticity, and appropriate certification as provided under the relevant legal provisions. Health information should be protected completely from access by confidentiality, integrity and access controls that are defined by the Health Insurance Portability and Accountability Act (HIPAA) under Bill of Rights (U.S.A.) for such information protection. Right to erasure: the so-called right to oblivion is one of the most stringent according to the European General Data Protection Regulation on data protection. From this perspective, it might create some understanding problems for the immutable records of the blockchain. While the Digital Personal Data Protection Bill, 2023, is operational in India, it lays down criteria for consented access, legal processing of data and protection against unauthorized use of health record systems on blockchain.[10] The collection, preservation and exhibition of digital evidence during the investigation and trial process are the domain of the Bharatiya Nagarik Suraksha Sanhita (BNSS) and the respective other criminal procedural laws of India. Such laws shall be adhered to in order to ensure the application of relevant digital forensic techniques in putting an evidential basis on the blockchain records in the court.



Fig 2: Legal framework for Blockchain Health record

A. Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023, affects the legal weight of blockchain-based health records during court proceedings. Such records need to fulfil particular statutory and technical requirements for their admissibility in courts, which prove their reliability, credibility and legal efficacy.[11]

Integrity of Records

The data must be intact, tamper-proof and unaltered. Blockchain technology inherently ensures this by cryptographic hash functions which give unique identifiers to each block of data and consensus mechanisms for validating transactions across distributed nodes. It is important to detect any unauthorized modification immediately to preserve the evidentiary integrity.

Authenticity Of Origin and Time

The courts require evidence to establish the dates of creation for digital records and their documented sources. Blockchain technology provides secure authentication through digital signatures which prove the identity of data creators and permanent timestamps which establish the exact time and place of record creation and record updates. The system offers custody link verification which supports medical legal cases by validating evidence authenticity while detecting structural problems because even minor inconsistencies can lead to case outcome changes.

Certification and Compliance

The evidentiary strength of blockchain platforms requires certification from recognized authorities or auditors who serve as trustworthy entities. The certification process verifies security protocols and operational effectiveness while checking compliance with both industry standards and legal requirements of the Digital Personal Data Protection Act 2023. The certification process establishes judicial trust in blockchain record evidence while making it less likely for opposing parties to dispute the evidence.

B. Information Technology Act, 2000

The Information Technology (IT) Act of 2000 establishes the primary legal framework which governs procedures for electronic document handling and digital signature authentication and information security protection methods used throughout the nation. The legislation establishes a legal framework to validate electronic transactions while safeguarding all types of digital information therefore it serves as an essential requirement for implementing blockchain technology in healthcare settings.[12] The requirements including those upon which the Project must not be deviated from must all apply to each participant consociate who will handle the project execution throughout their entire project work.

Legal Recognition of Electronic Signatures

The Act establishes an authentication procedure for electronic signatures and digital signatures and electronic records according to Sections 3 and 5. Digital signatures function as a security element within blockchain transaction systems to verify the identity of healthcare providers and institutions and their patients which produces legal proof that matches the value of handwritten signatures. The system plays a crucial role in determining whether blockchain-stored consent forms and prescriptions and medical entries hold authentic value as evidence.

Data Security Obligations

The IT Act 2000 establishes essential requirements for handling sensitive personal data through its Section 43A rules and regulations. The Act requires organizations to establish security measures through their security protocols and systems.

The blockchain technology-based health records achieve their best implementation through three specific attributes which include encryption and distributed storage and access control that blockchain technology inherently provides. Regulations create stronger data protection because they establish trust in blockchain records which prove their actual legal identity.

Liability for Data Breaches

The Act establishes organizational accountabilities for all improper financial outcomes which result from their failure to implement proper security protocols. Medical record breaches in the health sector create patient damage and result in hospitals and service providers facing legal responsibilities. The blockchain system protects against unauthorized access because it operates through a design that prevents any alterations yet organizations that implement blockchain technology must comply with IT Act rules to avoid legal liability.legal.

C. Digital Information Security in Healthcare Act (Disha)

The Digital Information Security in Healthcare Act (DISHA) is still a draft, but it is poised to serve as a specialized legal framework for the protection of health information in India. The law will become a crucial legal document which establishes essential rules for protecting personal information and securing digital health record systems. The DISHA Act contains essential provisions which directly support the implementation of blockchain technology within the healthcare industry.[13]

Data Privacy

The Digital Information Security in Healthcare Act establishes patient data rights through its specific regulations which govern health data collection, storage, processing, and sharing. Patients can create their own privacy protection methods because blockchain permits decentralized control through smart contracts that enable them to decide who can access their medical records at particular times.

Data Security

Healthcare organizations must develop strong cybersecurity systems which will safeguard health data from unauthorized access according to legal requirements. The permanent record function of blockchain technology together with its cryptographic encryption system and access control mechanisms helps organizations achieve their legal obligations while protecting against both inside security threats and outside tampering attempts.

Data Breach Notification

The DISHA regulation establishes mandatory breach notification rules which require healthcare providers to inform both patients and government authorities about security breaches. The blockchain technology provides better breach detection and reporting capabilities because its real-time audit trails and verifiable logs system reduce the risk of security incidents being reported after they occur.

Data Portability

DISHA establishes a fundamental patient right which enables them to obtain their medical records from all healthcare facilities. The interoperability of blockchain with prescriptive networks enables secure data transfer between healthcare systems which supports ongoing patient treatment while letting patients maintain control over their medical records.

All courts in every nation, including Indian courts, now recognize blockchain records as valid proof, provided that proper authentication methods for the records are established. The three elements of immutability and timestamping and verifiability serve as reliable indicators for jurisdictions that accept blockchain technology to assess its authenticity.

The current situation shows that organizations use blockchain technology to demonstrate their adherence to electronic evidence standards because there are no complete laws which define which types of evidence should be accepted in court.

The legal system will probably see future changes which will impact how blockchain technology is used for evidence collection in cases which involve medical disputes based on the jurisdictional boundaries between different medical specialties.

IV. CONCLUSION

The availability of authentic medical records will determine the success of quality healthcare delivery and the reduction of potential legal risks because traditional systems create security weaknesses that enable data breaches and unauthorized modifications. The unchangeable nature of blockchain with its decentralized structure and transparent operations and smart contract features provides organizations with secure solutions. The contemporary legal challenges of modern society make permission blockchain systems the least effective method for resolving legal disputes because they fail to achieve a balance between privacy protection and compliance requirements and user accessibility.

The proposed measures will achieve compliance with the Bharatiya Sakshya Adhiniyam 2023 law and its associated regulations, HIPAA, GDPR, and India's Digital Personal Data Protection Act, 2023. Judges are becoming more comfortable with blockchain evidence, yet its legal status remains undecided. The adoption process depends on four factors which include scalability and integration and cost and trust, whereas pilot projects will determine optimal practices for the process.

The healthcare industry can benefit from blockchain technology, which improves data integrity and consent management and evidence reliability, although it does not provide a complete solution.

REFERENCES

- [1] Snoswell, Centaine L, Smith, Anthony C, et.al., V Video and Phone Consultations Only Scratch the Surface of What Telehealth Has to Offer 765-771 (The Conversation Media Trust, Manchester, 8th edn., 2020).
- [2] Frick, Nicholas RJ, Mirbabaie, Milad, et.al., “Maneuvering Through the Stormy Seas of Digital Transformation: The Impact of Empowering Leadership on the AI Readiness of Enterprises” 30(2-3) *Journal of Decision Systems* 235-258 (2021).
- [3] Dmitrii Kolpashchikov and Olga Gerget, “Robotics and Artificial Intelligence in Healthcare”, in Roman Meshcheryakov (ed.), *Advances in Intelligent Healthcare Delivery and Management* 93-106 (Springer, 9th edn., 2024).
- [4] Georgiou, Konstantinos E, Georgiou, Evangelos, et.al., “5G Use in Healthcare: The Future is Present” 25 *JSLs: Journal of the Society of Laparoscopic & Robotic Surgeons* 4-8 (2021).
- [5] Mirbabaie, Milad, Stieglitz, Stefan, et.al., “Understanding Collaboration with Virtual Assistants--The Role of Social Identity and the Extended Self” 63 *Business & Information Systems Engineering* 21-37 (2017).
- [6] Ishwar Ahuja and Sakina Kapadia, “Digital Personal Data Protection Act, 2023 – A Brief Analysis” 1 *Bar & Bench* 30-31 (2023).
- [7] Clark, Robyn A, Inglis, Sally C, et.al., “Telemonitoring or Structured Telephone Support Programmes for Patients with Chronic Heart Failure: Systematic Review and Meta-Analysis” 334(76) *Bmj* 942-948 (2007).
- [8] Greenhalgh, Trisha, Kristjansson, Elizabeth, et.al., “Realist Review to Understand the Efficacy of School Feeding Programmes” 335(76) *Bmj* 858-861 (2007).
- [9] Andrews J.G., Buzzi S., Choi W., Hanly S.V., Lozano A., Soong A.C., Zhang J.C. What will 5G be? *IEEE J. Sel. Areas Commun.* 2014;32:1065–1082.
- [10] Latif, Siddique, Qadir, Junaid, et.al., “How 5G Wireless (And Concomitant Technologies) Will Revolutionize Healthcare?” 9(4) *Future Internet* 93-98 (2017).
- [11] Soldani, David, Fadini, Fabio, et.al., VI 2017 IEEE 85th Vehicular Technology Conference (VTC Spring) 1-5 (Ieee, Manchester, 3rd edn., 2017).
- [12] Zhang, Yangan, Chen, Guichen, et.al., IX *Electronics* 17-53 (Mdpi, Toronto, 5th edn., 2020).
- [13] Harshit Bhimrajka, “Insight on Digital Information Security in Healthcare Act, 2018” 1 *Digital Health* 3-4 (2020).