



ORIGINAL

An Overview of Blockchain-Based Electronic Health Records and Compliance with GDPR and HIPAA

Una visión general de los historiales médicos electrónicos basados en Blockchain y el cumplimiento del GDPR y la HIPAA

Nehal Ettaloui¹, Sara Arezki¹, Taoufiq Gadi¹

¹Faculty of science and techniques, Hassan First University Settat, Morocco.

Cite as: Ettaloui N, Arezki S, Gadi T. An Overview of Blockchain-Based Electronic Health Records and Compliance with GDPR and HIPAA. Data and Metadata. 2023;2:166. <https://doi.org/10.56294/dm2023166>


Submitted: 31-08-2023

Revised: 06-11-2023

Accepted: 29-12-2023

Published: 30-12-2023

Editor: Prof. Dr. Javier González Argote 

Guest Editor: Yousef Farhaoui 

Note: Paper presented at the International Conference on Artificial Intelligence and Smart Environments (ICAISE'2023).

ABSTRACT

The healthcare sector plays a pivotal role in both generating and relying on vast amounts of data, emphasizing the significance of collecting, managing, and sharing information. Technological advancements have facilitated the transformation of healthcare data into electronic health records (EHRs). These digital records are disseminated among various stakeholders, including patients, healthcare professionals, providers, insurance companies, and pharmacies. Given the sensitivity of healthcare information, the assimilation of new technologies is paramount. Blockchain technology, with its immutable nature and decentralized features, has emerged as a promising solution to instigate changes in the healthcare system. In the healthcare domain, where confidentiality is crucial, strict regulations are in place to safeguard patient privacy. Frameworks like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) are designed to mitigate the risks associated with health data breaches. Although blockchain's characteristics, such as enhanced interoperability, anonymity, and access control, can improve the overall landscape of health data management, it is imperative for blockchain applications to adhere to existing regulatory frameworks for practical implementation. This paper delves into the examination of the compliance of blockchain-based EHR systems with regulations like HIPAA and GDPR. Additionally, it introduces a Blockchain-based EHR model specifically crafted to seamlessly align with regulatory requirements, ensuring its viability and effectiveness in real-world scenarios.

Keywords: Blockchain; Healthcare; Electronic Health Record; GDPR; HIPAA; Hyperledger Fabric; IPFS.

RESUMEN

El sector sanitario desempeña un papel fundamental tanto en la generación como en la utilización de grandes cantidades de datos, lo que pone de relieve la importancia de recopilar, gestionar y compartir la información. Los avances tecnológicos han facilitado la transformación de los datos sanitarios en historiales médicos electrónicos (HCE). Estos registros digitales se difunden entre diversas partes interesadas, como pacientes, profesionales sanitarios, proveedores, compañías de seguros y farmacias. Dada la sensibilidad de la información sanitaria, la asimilación de las nuevas tecnologías es primordial. La tecnología Blockchain, con su naturaleza inmutable y sus características descentralizadas, ha surgido como una solución prometedora para instigar cambios en el sistema sanitario. En el ámbito sanitario, donde la confidencialidad es crucial, existen normas estrictas para salvaguardar la privacidad de los pacientes. Marcos como el Reglamento General de Protección de Datos (RGPD) y la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) están diseñados para mitigar los riesgos asociados a las violaciones de datos sanitarios. Aunque las características

de blockchain, como la interoperabilidad mejorada, el anonimato y el control de acceso, pueden mejorar el panorama general de la gestión de datos sanitarios, es imperativo que las aplicaciones de blockchain se adhieran a los marcos normativos existentes para su aplicación práctica. Este documento profundiza en el examen de la conformidad de los sistemas de HCE basados en blockchain con normativas como HIPAA y GDPR. Además, presenta un modelo de HCE basado en Blockchain diseñado específicamente para adaptarse sin problemas a los requisitos normativos, garantizando su viabilidad y eficacia en situaciones reales.

Palabras clave: Blockchain; Sanidad; Historia Clínica Electrónica; GDPR; HIPAA; Hyperledger Fabric; IPFS.

INTRODUCTION

Blockchain-based EHR are emerging as a transformative solution for the secure and streamlined storage and sharing of Patient Health Information (PHI) in the healthcare sector. The decentralized and immutable nature of blockchain technology, while holding great promise, introduces distinctive challenges in aligning with stringent privacy and security regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR).⁽¹⁾

HIPAA and GDPR stand as pivotal regulations governing the entire lifecycle of EHR, encompassing its collection, usage, and disclosure. Compliance with these regulations is not only a legal imperative but also foundational to upholding the privacy and security of PHI. Moreover, it plays a crucial role in fostering trust among patients and healthcare providers in the incorporation of technology within healthcare practices.

This article undertakes an in-depth exploration of the intricacies involved in achieving compliance with HIPAA and GDPR in the context of blockchain-based EHRs. It aims to provide organizations with comprehensive insights into the multifaceted steps required to synchronize regulatory adherence with the unique features and advantages offered by blockchain technology. Additionally, the discussion delves into the potential ramifications of non-compliance, elucidating the impact on patients, healthcare providers, and organizational stakeholders.

By delving into the specific challenges and nuances associated with achieving compliance in the realm of blockchain-based EHRs, this article seeks to equip healthcare organizations with tailored strategies and best practices. These approaches are essential not only for meeting regulatory requirements but also for leveraging the transformative potential of blockchain technology. The overarching goal is to enhance the efficiency and security of healthcare data while maintaining the utmost standards of privacy and security for EHR.⁽²⁾

Blockchain

Blockchain technology harbors transformative potential in the healthcare sector by enabling the creation of secure and decentralized EHRs. This innovation empowers patients, providing them with control over their health information while concurrently enhancing the accuracy and accessibility of medical data.⁽³⁾

In understanding how blockchain operates, the fundamental process involves a decentralized network of computers, or nodes. As illustrated in figure 1, A healthcare transaction within this blockchain ecosystem follows a systematic sequence. It begins with the initiation of a healthcare transaction, whether it involves updating a patient's health record or creating a new entry. The transaction undergoes rigorous verification through consensus mechanisms like proof-of-work or proof-of-stake to ensure its legitimacy. Once verified, the transaction is grouped into a new block, with each block containing a unique cryptographic hash linking it to the preceding one. The network then achieves consensus on the validity of the new block, crucial for maintaining the integrity of the entire blockchain. The validated block is seamlessly appended to the existing blockchain, creating an immutable and transparent ledger distributed across all nodes.⁽⁴⁾

The cryptographic security features of each block, including a unique signature, ensure the security and immutability of the data. Any attempt to tamper with a block would necessitate altering all subsequent blocks, making the blockchain highly resistant to fraudulent activities.

In terms of blockchain types, there are two primary categories: Public and Private. Public blockchains, exemplified by Bitcoin and Ethereum, offer open accessibility, participation, and transparency. They are ideal for applications where a high degree of decentralization is essential. On the other hand, Private or permissioned blockchains restrict access and participation to a predetermined group of participants. Despite existing challenges, ongoing development and exploration of blockchain applications in healthcare hold the promise of not only overcoming these hurdles but also unlocking the full potential of this revolutionary technology for transforming health data management.⁽⁵⁾

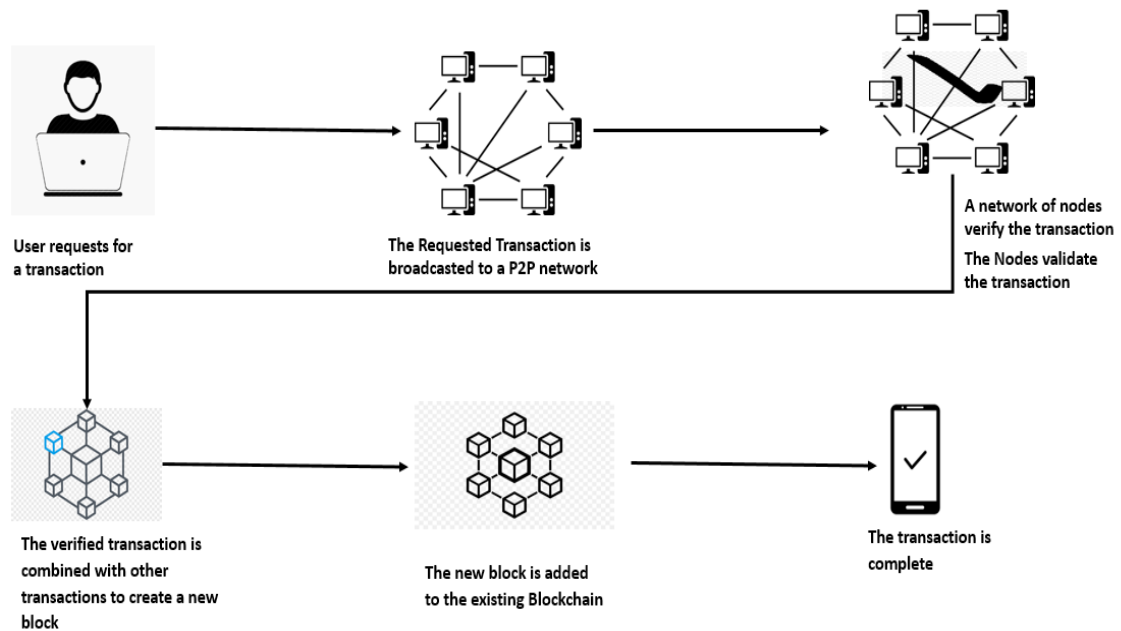


Figure 1. Steps of blockchain transaction

Blockchain-Based EHR

Implementing blockchain technology in EHRs enhances both security and accessibility. This empowers patients to exercise control over who can access and modify their health data. Meanwhile, healthcare providers benefit from streamlined access to accurate and real-time medical information, thereby minimizing the risk of medical errors and enhancing overall patient outcomes.⁽⁶⁾

Beyond its fundamental role in securing health information, blockchain-based EHRs open avenues for advancing global medical research and improving public health outcomes. With patient consent, researchers gain access to anonymized health data stored on the blockchain, fostering the development of innovative treatments and a deeper understanding of diseases.⁽⁷⁾

Despite the promising potential of blockchain in healthcare, the widespread adoption of blockchain-based EHRs is still in its infancy. Significant challenges, such as compliance with health regulations, interoperability between diverse EHR systems and the standardization of data formats, need to be overcome. Nonetheless, the transformative capabilities of blockchain technology suggest a promising future, revolutionizing how health data is stored, shared, and utilized.⁽⁸⁾

General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a regulation passed by the European Union in May 2016 to protect the privacy and personal data of citizens. The GDPR replaces the 1995 Data Protection Directive and came into effect on May 25, 2018. The GDPR sets out rules for how organizations must handle personal data, including how it is collected, used, processed, and stored. It also gives individuals more control over their personal data and provides them with greater rights, including the right to access their data, the right to have their data erased, and the right to object to the processing of their data. The GDPR applies to any organization that processes the personal data of EU citizens, regardless of where the organization is located. Failure to comply with the GDPR can result in significant fines and penalties.⁽⁹⁾ The General Data Protection Regulation (GDPR) is a set of rules established by the European Union (EU) to protect the privacy and personal data of its citizens. Some of the key rules of GDPR include:⁽¹⁰⁾

- **Consent:** It is imperative for data controllers to secure explicit and precise consent from individuals for the processing of their personal data. This consent should be freely given, unambiguous, and well-informed.
- **Right to access:** Individuals possess the entitlement to be informed about the collection, processing, and storage of their personal data.
- **Right to erasure:** Individuals retain the right to request the deletion or erasure of their personal data.
- **Data portability:** Individuals have the right to receive a structured, machine-readable copy of their personal data and the ability to transmit this information to another controller.
- **Privacy by design:** Data controllers are obligated to incorporate technical and organizational measures that embed data protection principles into the design of their systems and processes.

Health Insurance Portability and Accountability Act

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. It is a federal law in the United States that aims to protect the privacy and security of individuals' personal health information (PHI).⁽¹¹⁾

The main objectives of HIPAA are to ensure the confidentiality and security of PHI, limit the access and use of PHI to authorized individuals, provide individuals with rights over their PHI and establish standards for the electronic exchange of PHI. HIPAA applies to all health care providers, health plans, and health care clearinghouses that electronically transmit health information. The law requires these covered entities to implement safeguards to protect the privacy and security of PHI and to comply with specific regulations related to PHI, such as the HIPAA Privacy Rule and the HIPAA Security Rule. HIPAA violations can result in significant penalties, including fines and legal action. Individuals can file complaints with the U.S. Department of Health and Human Services if they believe their rights under HIPAA have been violated.

HIPAA has two main rules that govern the use and disclosure of protected health information (PHI). These rules are:⁽¹²⁾

- **HIPAA Privacy Rule:** This rule sets national standards for protecting the privacy of PHI. It establishes guidelines for how covered entities can use, disclose, and safeguard PHI, as well as the rights of individuals to access and control their PHI. The Privacy Rule also requires covered entities to appoint a privacy officer, train their workforce on privacy practices, and implement administrative, physical, and technical safeguards to protect PHI.
- **HIPAA Security Rule:** This rule establishes national standards for securing electronic PHI (ePHI). The Security Rule requires covered entities to implement administrative, physical, and technical safeguards to protect ePHI from unauthorized access, use, and disclosure. It also requires covered entities to implement policies and procedures for responding to security incidents and to conduct periodic risk assessments to identify and mitigate potential vulnerabilities.

In addition to the Privacy and Security Rules, HIPAA also includes provisions related to breach notification, enforcement, and penalties for non-compliance.

Literature Review

The EHR landscape has witnessed a substantial transformation due to advancements in healthcare technologies. This shift in the storage and management of patient information has prompted extensive research into data preservation systems, with blockchain technology emerging as a key player to enhance security and privacy.

In one such studies,⁽¹³⁾ introduced a customized system for preserving electronic medical records, utilizing blockchain to secure patient information. Similarly,⁽¹⁴⁾ proposed MedRec, another blockchain-based solution for managing medical records. However, both approaches encountered difficulties on public blockchains, especially in managing sensitive data such as health records, and raised concerns regarding GDPR compliance. Additionally, neither system adequately tackled scalability issues inherent in the extensive health sector data.⁽¹⁵⁾ suggested Ancile, an Ethereum-based system, without adhering to GDPR principles and overlooking scalability issues. A study⁽¹⁶⁾ Fabric-based system with an incentivized model for sharing and storing medical privacy data was presented, but it fell short in providing complete control to patients over their data and lacked compliance with GDPR and HIPAA rules, crucial for protecting patient rights and ensuring secure handling of sensitive health information.

Wang et al.⁽¹⁷⁾ presented a decentralized access control approach based on secret policy attribute encryption combined with an Ethereum public chain. However, this approach increased the burden on chain storage and the responsibilities of data owners.

In contrast, our proposed model adopts a privacy-centric approach by implementing a permissioned blockchain based on the Hyperledger Fabric solution. This ensures that only authorized participants can access the data, thereby enhancing confidentiality levels. Furthermore, we address scalability challenges by integrating IPFS, facilitating seamless storage of substantial volumes of authentic medical data.

In overcoming the limitations of existing solutions, our model stands out. Our approach prioritizes GDPR compliance by respecting the right to be forgotten and minimizing on-chain data. Compared to a study,⁽¹⁶⁾ our model introduces an incentive system while maintaining decentralization. In contrast to a study,⁽¹⁷⁾ it mitigates storage burden and simplifies data owner responsibilities through innovative solutions like IPFS integration. Ultimately, our proposed model offers a more robust, secure, and scalable option for managing electronic medical records, aligning with contemporary privacy and compliance requirements.

RESULTS

Contradiction of blockchain-based EHR with GDPR

There are some potential contradictions between blockchain-based EHRs and the General Data Protection Regulation (GDPR).⁽¹⁾

One of the primary challenges is the right to be forgotten, which is a fundamental principle of the GDPR. This principle gives individuals the right to have their personal data erased, which can be difficult to implement in a blockchain-based system, as the technology is designed to create a tamper-proof, immutable record of data. Once data has been added to a blockchain, it cannot be easily deleted or modified, which could conflict with the right to be forgotten.

Another issue is the GDPR's requirement for data minimization, which requires that only the minimum amount of personal data necessary for a specific purpose is collected and processed. In a blockchain-based EHR system, all information is recorded on the blockchain, which could lead to an excessive amount of data being collected and processed, potentially violating the GDPR's data minimization principle.

Furthermore, the GDPR requires that personal data is processed lawfully, fairly, and transparently. The use of blockchain technology could potentially make it difficult for patients to understand how their data is being processed and who has access to it, which could conflict with the GDPR's transparency requirement.⁽¹⁰⁾

Contradiction of blockchain-based EHR with HIPAA

There are potential contradictions between blockchain-based EHRs and the Health Insurance Portability and Accountability Act, for the protection of individuals' medical records and other personal health information.⁽¹⁸⁾

One of the primary challenges is the requirement under HIPAA for covered entities to ensure the confidentiality, integrity, and availability of PHI. While blockchain technology can provide secure storage and transmission of PHI, there are concerns about the transparency of blockchain-based systems and the potential for unauthorized access to PHI. This could potentially conflict with the confidentiality requirement under HIPAA.

Another challenge is the HIPAA requirement for covered entities to have agreements in place with business associates that handle EHR, to ensure that the business associates also comply with HIPAA. It may be difficult to ensure that all parties involved in a blockchain-based EHR system are compliant with HIPAA, as the decentralized nature of the blockchain means that it may be difficult to identify all parties that have access to PHI.

Additionally, the HIPAA Security Rule requires covered entities to have reasonable and appropriate administrative, physical, and technical safeguards to protect PHI. It may be difficult to ensure that blockchain-based EHR systems have adequate safeguards in place, as the technology is still relatively new and may not have established best practices for security and privacy.

Outlined solutions for ensuring Blockchain-based EHR compliance with GDPR and HIPAA

To achieve thorough adherence to both GDPR and HIPAA, our suggested measures encompass a range of strategic approaches:

- **Off-Chain Storage (IPFS):** Leverage IPFS or similar distributed storage systems to align with GDPR's right to erasure and rectification and addresses HIPAA's data minimization requirement. Storing sensitive patient data off-chain while preserving only hashes or references on the blockchain allow seamless modification or deletion without compromising integrity.^(9,12)
- **Cryptography:** Implementing advanced encryption methods through cryptography significantly enhances data security. Prior to storage off-chain, patient information is encrypted, making it unreadable without the corresponding decryption keys. To ensure data integrity and facilitate authenticity verification without exposing the actual data, cryptographic hashes are employed on the blockchain. This approach is in strict accordance with the security standards outlined by both GDPR and HIPAA.^(10,13)
- **Patient Consent Management:** Employing smart contracts to manage patient consent effectively, enable precise control over data access. These contracts empower patients to grant or revoke consent as needed, regulating access to their medical records. Maintain a transparent access log through smart contracts, recording all data access requests and approvals to establish a robust audit trail for GDPR compliance.⁽¹¹⁾ This also aligns with HIPAA's requirement for strict access controls.
- **Data Minimization and Segmentation:** Leverage off-chain storage and smart contracts for data minimization. Adopt data segmentation strategies to store only relevant information on the blockchain, with minimal patient identifiers or data summaries. This targeted approach directly addresses HIPAA's data minimization requirement while optimizing storage efficiency.⁽¹²⁾
- **Data Portability Measures:** Implement mechanisms for data portability as mandated by GDPR. Enable patients to request their data and, upon consent, receive cryptographic keys to access their encrypted information stored off-chain. This ensures compliance with GDPR's emphasis on empowering individuals to control and transfer their personal data.⁽¹⁹⁾
- **Private Blockchain:** Evaluate the use of private blockchain where access is restricted to authorized participants. This aligns with the permissioned blockchain model and facilitates compliance with both HIPAA and GDPR by controlling data access and ensuring a trusted network.⁽²⁰⁾
- **Standardization and Interoperability:** Advocate for industry-wide standards and interoperability

protocols that align with both blockchain technology and regulatory requirements. This could streamline data exchange between different EHR systems and enhance overall compliance.

By integrating these advanced solutions, the blockchain-based HER system not only addresses the challenges posed by GDPR and HIPAA individually but also sets a new standard for secure and ethical electronic medical record management that aligns seamlessly with both regulatory frameworks.

Proposed Model for Ensuring GDPR and HIPAA Compliance in Blockchain-Based EHR Systems

In this section, we will introduce the envisioned model architecture as presented in figure 2, seamlessly integrating meticulous and supervised data access control to empower patients with extensive command over their private information through the implementation of chaincode. Employing Hyperledger Fabric and off-chain storage via IPFS, the system's elevated architecture encompasses pivotal elements such as identity management, decentralized data storage, blockchain-driven access control, and immutable provenance.⁽²¹⁾ In alignment with GDPR terms, patients and healthcare providers assume vital roles. The secure storage of EHR on decentralized IPFS, coupled with their linkage to digital identities, ensures validation for access by data processors through blockchain-based protocols.⁽²²⁾

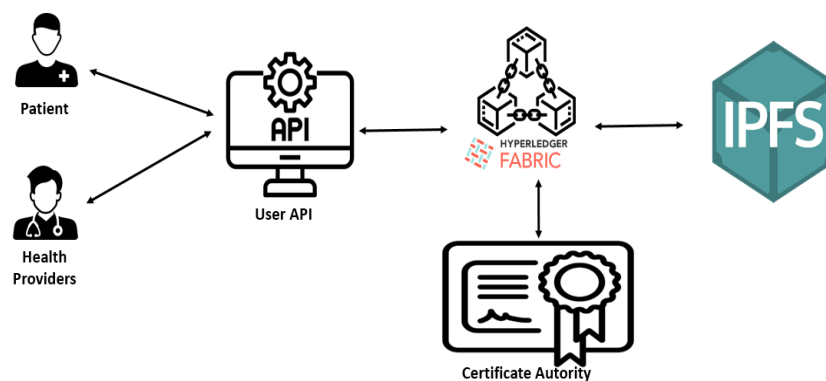


Figure 2. Architecture of the proposed model

Participants

Within the system, participants are categorized into two main roles: Patient nodes and Healthcare Providers nodes. Patient nodes oversee web-connected devices, collecting diverse medical data at regular intervals and transmitting this information securely. The gathered data is encrypted before being sent to the IPFS. Patient also have the capability to execute smart contracts. Healthcare Providers nodes deliver continuous healthcare services, utilizing medical data that includes encrypted EHRs, encompassing diagnoses, laboratory reports, and insurance documents. Similar to Patient nodes, Healthcare Providers nodes possess functionalities related to blockchain operations. Both types of participants access the blockchain network through a client application ensuring efficient interaction within the system.

Hyperledger fabric Blockchain

The Hyperledger blockchain serves as the foundational element of our model, with all users in healthcare sector undergoing registration within the Hyperledger-based blockchain network to access the provided services. Access privileges for participants, or healthcare providers are determined by an access control list, which is both stored on and implemented through smart contracts on the Hyperledger blockchain. Importantly, only metadata, not the full data, is stored on the blockchain. This ensures that access to the blockchain is governed by predefined rules within the Hyperledger framework while maintaining efficiency by storing only essential information on the chain. The Hyperledger blockchain not only guarantees data provenance and tracking but additionally enables the recording of transactions and Ensures that participants are held accountable for their actions. This robust framework, based on Hyperledger technology, enhances transparency, security, and reliability within the smart healthcare ecosystem.

IPFS

IPFS is utilized for storing diverse health data, including reports, prescriptions, and critical medical history. Sensitive information is securely stored off-chain, ensuring compliance with GDPR's "Right to be Forgotten" rule and providing data owners with full control. Off-chain storage also reduces the cost of storing data on the blockchain. The process involves encrypting data using a symmetric key, which is further encrypted with the owner's public key and stored on IPFS. Only hashes of off-chain data is recorded within blockchain.

Smart contracts (Chaincode)

Implemented on the blockchain, smart contracts or chaincode using Hyperledger terminology, are activated by participants within the blockchain to execute specific tasks. These contracts are intricately designed to deliver authentication, authorization, access control, and transaction logging on the blockchain. The chaincode encapsulates three primary functionalities. Initially, it empowers the device owner to exercise control over the data and streaming through a well-defined set of rules. Secondly, participants utilize the smart contract to facilitate data sharing within the network. Lastly, the owner employs the smart contract to delegate data access control to authorized nodes, ensuring a secure and controlled data-sharing environment.

Access Control, and Secure Data Transactions

Patients exercise precise control over their medical records, dictating permissions for stakeholders in a regulated environment. This control extends to reading, writing, or denying access, ensuring comprehensive ownership and authority. Patients can authorize access based on predefined roles and permissions for authenticated users. They also have the authority to deny specific physicians access, preventing the release of records to other medical professionals.

Smart contracts play a crucial role in orchestrating interactions within the user-system paradigm. They identify and validate requests, manage record updates, and administer access permissions.

Upon patient authorization, healthcare providers can generate and encrypt health records, storing them in IPFS while securing the hash value within the Hyperledger blockchain. If patients grant access for record modifications, a transient, patient-centric view is created. Subsequently, the healthcare providers updates this view, and upon patient endorsement, both the IPFS-stored record and the Health record chain undergo a permanent update. To enable stakeholder access, patients can grant retrieval access, allowing retrieval of partial, attribute-based information from IPFS using the hash value within the Health record chain network.

Evaluation and comparison with existing solutions. Data Ownership

Patients as data owners have the exclusive authority to conduct CRUD operations on their data, reinforcing crucial rights like the "Right to Access" and "Right to Rectification." The utilization of chaincode further ensures compliance with HIPAA, enforcing a request and access policy before disseminating health data to external parties. This approach not only aligns with HIPAA's access control requirements but also emphasizes the model's dedication to safeguarding the privacy and security of sensitive healthcare records.

The comprehensive access granted to data owners facilitates their oversight of data usage, embodying the "Right to Restricted Processing" and the "Right to Data Portability"—integral aspects of HIPAA compliance. This model not only upholds fundamental data ownership rights but also aligns seamlessly with the stringent regulations set by HIPAA, ensuring a secure, transparent, and compliant approach to managing health-related data.

Off-chain storage

Data erasure on IPFS is meticulously designed to comply with the "Right to be Forgotten" principle and aligns notably with HIPAA. HIPAA compliance is emphasized through data owners' retained control to delete their information on IPFS, ensuring adherence to HIPAA's regulations on Protected Health Information control. Additionally, the blockchain remains free of personal data, reinforcing compliance with HIPAA's stringent privacy standards.

Off-chain storage of critical information in the IPFS database, alongside secure removal facilitated by smart contracts, further solidifies the model's commitment to GDPR and HIPAA compliance. This meticulous approach ensures a secure and compliant framework for health-related data management.

Authentication

Authentication is a pivotal component of the proposed solution, grounded in a permissioned blockchain that adopts a secure identity-based approach. This robust authentication process is designed to comply with both HIPAA and GDPR, ensuring the secure handling of sensitive health data.

Participants, before engaging in activities like uploading, accessing, or sharing health data, undergo mandatory registration on the network. Verification of all participants and stakeholders within the healthcare system is meticulously managed through a trusted Certificate Authority (CA) and a standard identity management system. This strict authentication protocol aligns with the stringent access control requirements of both HIPAA and GDPR, prioritizing data security and privacy in healthcare data management.

All transactions within the private healthcare network are digitally signed at the proposal stage, ensuring a robust authentication of identities. This comprehensive measure not only enhances data security but also fulfills the authentication standards mandated by both HIPAA and GDPR. The prototype implementation leverages Hyperledger Fabric service's Membership Service Provider, further elevating the effectiveness of

identity management and aligning with recommended practices for secure healthcare data handling.

Privacy by design

The proposed framework prioritizes privacy by design, aligning seamlessly with both HIPAA and GDPR. Following the principles outlined in GDPR, the framework incorporates privacy considerations right from the design phase, showcasing a commitment to secure and compliant handling of sensitive health data.

In adherence to GDPR and HIPAA standards, Personally Identifiable Information and sensitive data are intentionally stored on the IPFS, emphasizing the framework's dedication to stringent privacy practices. This deliberate approach ensures that sensitive information, such as Protected Health Information, is securely managed, aligning with HIPAA's emphasis on safeguarding health-related data.

The framework facilitates controlled sharing of private data among participants through smart contracts, underscoring confidentiality with off-chain data storage and secure sharing mechanisms. By restricting access to chaincode and transactions exclusively to network participants, the framework ensures privacy within the permissioned network. This comprehensive privacy strategy not only meets GDPR's privacy-by-design requirements but also aligns with HIPAA's rigorous standards, establishing a robust foundation for the secure and compliant management of health-related data.

Traceability

Traceability is a cornerstone feature of the proposed framework, designed with meticulous attention to compliance with both HIPAA and GDPR. The framework's commitment to traceability not only instills trust in the system but also ensures a secure and compliant approach to managing sensitive health data.

To achieve this, the framework incorporates a robust traceability mechanism by securely storing data logs on the blockchain ledger. Leveraging the immutability of the blockchain, this practice aligns with both HIPAA and GDPR standards, providing an unalterable record of changes in data, data requests, data sharing, and other transactions related to data. This unalterable record on the blockchain serves as a valuable resource for tracking data, whether for forensic purposes or other investigative needs.

By adhering to the principles of both regulatory frameworks, the framework not only instills confidence in the integrity of the system but also ensures that traceability requirements are met comprehensively. This approach reflects the commitment to secure, transparent, and compliant data management practices, aligning with the expectations outlined in both HIPAA and GDPR.

Comparison with existing solution:

Delivering enhanced security, privacy, and scalability, our proposed model surpasses existing frameworks outlined in Table 1. While numerous privacy-preserving methods target specific aspects, they often fall short in providing a comprehensive strategy to address the concerns of diverse stakeholders. This encompasses alignment with user preferences, adherence to regulations, and the resolution of Single Points of Failure.

In contrast to systems akin to our model, which extend beyond addressing basic data sharing challenges, our approach systematically confronts additional complexities. This includes ensuring compliance with privacy regulations and proficiently managing users' preferences. Furthermore, we advocate for the integration of Blockchain to meticulously record interactions among diverse stakeholders. This not only oversees the fulfillment of Privacy Agreement obligations but also broadens the system's scope.

Lastly, our system opts for IPFS, a distributed file system, for data storage, departing from the cloud storage approach used in a study.⁽¹⁸⁾ This strategic choice mitigates risks associated with Single Points of Failure and optimizes data retrieval latency. The distinctive features of our proposed model underscore its commitment to robust privacy, compliance, and efficient data management, marking a significant advancement in comparison to existing frameworks.

	Blockchain type	Storage	Patient Consent	Privacy concerns	Regulatory Compliance
(13)	Public Blockchain	On Chain	N	Y	N
(14)	Public Blockchain	On Chain	N	Y	N
(15)	Public Blockchain	Off Chain	Y	Y	N
(16)	Private Blockchain	Off Chain	N	Y	N
(17)	Public Blockchain	Off Chain	Y	Y	N
Our model	Private Blockchain	Off Chain	Y	Y	Y

CONCLUSION

In conclusion, the integration of blockchain-based electronic health records introduces nuanced challenges in aligning with the robust frameworks of HIPAA and GDPR regulations. As the healthcare sector progressively adopts blockchain technology, organizations are tasked with navigating the complexities of securing and preserving patient health information on the blockchain, all while adhering to the stringent requirements of these regulations. Achieving compliance in blockchain-based EHRs necessitates the development and implementation of comprehensive policies and procedures tailored to the unique demands of each regulation. This intricate process also mandates the integration of technical controls for safeguarding Protected Health Information (PHI) on the blockchain, the deployment of identity and access management solutions, the establishment of transparent user consent mechanisms, and the meticulous documentation of the compliance program.

Our proposed model seamlessly incorporates principles of permissioned blockchain, decentralized InterPlanetary File System storage, and smart contract-enabled consent management. This integrated approach aligns key stakeholders—patients, administrators, and doctors—with GDPR terminology, establishing a secure and auditable framework. This framework not only empowers patients, safeguarding their data privacy, but also streamlines regulatory adherence. The blockchain-based methodology not only addresses the intricacies of healthcare data compliance but also establishes the groundwork for a resilient and interoperable data management paradigm. This paradigm ensures the protection of sensitive information while fostering seamless data exchange within the healthcare domain.

Despite the inherent challenges associated with ensuring compliance in blockchain-based EHRs, maintaining the trust of patients and healthcare providers in the security and privacy of their Protected Health Information remains paramount. Organizations can successfully harness the benefits of blockchain technology by implementing essential measures to ensure compliance. This strategic approach not only fortifies the protection of PHI but also upholds compliance with both HIPAA and GDPR regulations, thereby ensuring the integrity and security of healthcare data in a rapidly evolving technological landscape.

REFERENCES

1. Hasselgren, P. K. Wan, M. Horn, K. Kralevska, D. Gligoroski, et A. Faxvaag, « GDPR Compliance for Blockchain Applications in Healthcare ». arXiv, 27 septembre 2020. Consulté le: 28 avril 2023. [En ligne]. Disponible sur: <http://arxiv.org/abs/2009.12913>
2. Zhou, M. Barati, et O. Shafiq, « A compliance-based architecture for supporting GDPR accountability in cloud computing », *Future Generation Computer Systems*, vol. 145, p. 104-120, août 2023, doi: 10.1016/j.future.2023.03.021.
3. Shahnaz, U. Qamar, et A. Khalid, « Using Blockchain for Electronic Health Records », *IEEE Access*, vol. 7, p. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.
4. H. S. A. Fang, T. H. Tan, Y. F. C. Tan, et C. J. M. Tan, « Blockchain Personal Health Records: Systematic Review », *J Med Internet Res*, vol. 23, no 4, p. e25094, avr. 2021, doi: 10.2196/25094.
5. Gonzalez-Argote J. Patterns in Leadership and Management Research: A Bibliometric Review. *Health Leadership and Quality of Life* 2022;1:10-10. <https://doi.org/10.56294/hl202210>.
6. Mohan, « State of Public and Private Blockchains: Myths and Reality », in *Proceedings of the 2019 International Conference on Management of Data*, in SIGMOD '19. New York, NY, USA: Association for Computing Machinery, juin 2019, p. 404-411. doi: 10.1145/3299869.3314116.
7. Romero-Carazas R. Prompt lawyer: a challenge in the face of the integration of artificial intelligence and law. *Gamification and Augmented Reality* 2023;1:7-7. <https://doi.org/10.56294/gr20237>.
8. X. Liu, Z. Wang, C. Jin, F. Li, et G. Li, « A Blockchain-Based Medical Data Sharing and Protection Scheme », *IEEE Access*, vol. 7, p. 118943-118953, 2019, doi: 10.1109/ACCESS.2019.2937685.
9. E. Chukwu et L. Garg, « A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations », *IEEE Access*, vol. 8, p. 21196-21214, 2020, doi: 10.1109/ACCESS.2020.2969881.
10. S. Srivastava, M. Pant, S. K. Jauhar, et A. K. Nagar, « Analyzing the Prospects of Blockchain in Healthcare Industry », *Comput Math Methods Med*, vol. 2022, p. 3727389, déc. 2022, doi: 10.1155/2022/3727389.

11. Auza-Santiváñez JC, Díaz JAC, Cruz OAV, Robles-Nina SM, Escalante CS, Huanca BA. mHealth in health systems: barriers to implementation. *Health Leadership and Quality of Life* 2022;1:7-7. <https://doi.org/10.56294/hl20227>.
12. R. Hussein et al., « General Data Protection Regulation (GDPR) Toolkit for Digital Health », *Stud Health Technol Inform*, vol. 290, p. 222-226, juin 2022, doi: 10.3233/SHTI220066.
13. M. Poelman et S. Iqbal, « Investigating the Compliance of the GDPR: Processing Personal Data On A Blockchain », in 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), janv. 2021, p. 38-44. doi: 10.1109/CSP51677.2021.9357590.
14. « Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC ». Consulté le: 28 avril 2023. [En ligne]. Disponible sur: <https://www.cdc.gov/phlp/publications/topic/hipaa.html>
15. W. Moore et S. Frye, « Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules », *J Nucl Med Technol*, vol. 47, no 4, p. 269-272, déc. 2019, doi: 10.2967/jnmt.119.227819.
16. Gonzalez-Argote J. A Bibliometric Analysis of the Studies in Modeling and Simulation: Insights from Scopus. *Gamification and Augmented Reality* 2023;1:5-5. <https://doi.org/10.56294/gr20235>.
17. H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, et S. Liu, « Blockchain-Based Data Preservation System for Medical Data », *J Med Syst*, vol. 42, no 8, p. 141, juin 2018, doi: 10.1007/s10916-018-0997-3.
18. Azaria, A. Ekblaw, T. Vieira, et A. Lippman, « MedRec: Using Blockchain for Medical Data Access and Permission Management », in 2016 2nd International Conference on Open and Big Data (OBD), août 2016, p. 25-30. doi: 10.1109/OBD.2016.11.
19. G. G. Dagher, J. Mohler, M. Milojkovic, et P. B. Marella, « Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology », *Sustainable Cities and Society*, vol. 39, p. 283-297, mai 2018, doi: 10.1016/j.scs.2018.02.014.
20. W. Zhan, C.-L. Chen, W. Weng, W.-J. Tsaur, Z.-Y. Lim, et Y.-Y. Deng, « Incentive EMR Sharing System Based on Consortium Blockchain and IPFS », *Healthcare (Basel)*, vol. 10, no 10, p. 1840, sept. 2022, doi: 10.3390/healthcare10101840.
21. « A Secure Cloud Storage Framework With Access Control Based on Blockchain | IEEE Journals & Magazine | IEEE Xplore ». Consulté le: 10 décembre 2023. [En ligne]. Disponible sur: <https://ieeexplore.ieee.org/document/8770246>
22. Gonzalez-Argote D, Gonzalez-Argote J, Machuca-Contreras F. Blockchain in the health sector: a systematic literature review of success cases. *Gamification and Augmented Reality* 2023;1:6-6. <https://doi.org/10.56294/gr20236>.
23. T.-F. Lee, I.-P. Chang, et T.-S. Kung, « Blockchain-Based Healthcare Information Preservation Using Extended Chaotic Maps for HIPAA Privacy/Security Regulations », *Applied Sciences*, vol. 11, no 22, Art. no 22, janv. 2021, doi: 10.3390/app112210576.
24. Hasselgren, K. Krlevska, D. Gligoroski, et A. Faxvaag, « GDPR Compliant Blockchain and Distributed Ledger Technologies in the Health Sector », *Stud Health Technol Inform*, vol. 270, p. 1293-1294, juin 2020, doi: 10.3233/SHTI200408.
25. G. Al-Sumaidae, R. Alkhudary, Z. Zilic, et A. Swidan, « Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare », *Information Processing & Management*, vol. 60, no 2, p. 103160, mars 2023, doi: 10.1016/j.ipm.2022.103160.
26. E. S. Babu, I. Kavati, S. R. Nayak, U. Ghosh, et W. Al Numay, « Secure and transparent pharmaceutical supply chain using permissioned blockchain network », *International Journal of Logistics Research and Applications*, vol. 0, no 0, p. 1-28, févr. 2022, doi: 10.1080/13675567.2022.2045578.

27. T. V. Doan, Y. Psaras, J. Ott, et V. Bajpai, « Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Directions ». arXiv, 2 avril 2022. doi: 10.48550/arXiv.2202.06315.

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

None.

AUTHORSHIP CONTRIBUTION

Conceptualization: Nehal Ettaloui, Sara Arezki, Taoufiq Gadi.

Research: Nehal Ettaloui, Sara Arezki, Taoufiq Gadi.

Drafting - original draft: Nehal Ettaloui, Sara Arezki, Taoufiq Gadi.

Writing - proofreading and editing: Nehal Ettaloui, Sara Arezki, Taoufiq Gadi.