Arizona State University

Ira. A. Fulton Schools of Engineering

The Polytechnic School

Information Technology

IFT 520 Advance Information Systems Security

DATA PRIVACY IN HEALTHCARE:

PROTECTING PATIENT DATA

Team 51:

Sanjay Pulluri (1232028735)

Archana Kanchimireddy (1232309145)

Sreeja Vaddi (1232211840)

Table of contents

1. ABSTRACT

Healthcare's digital revolution presents several privacy hazards that require careful consideration and preventative measures. This research looks at the various obstacles that the Internet of Things (IoT) and online medical data sharing present to the digitization of healthcare. To address these concerns, cooperation between patients, healthcare practitioners, and institutions is essential. It emphasizes the necessity of thorough privacy controls that address infrastructure security, data protection, and regulatory compliance. Then again, fresher advancements like virtual entertainment, wearables, and online hereditary information are not sufficiently covered by regulations like HIPAA. The report proposes updated regulations that are well-defined for the computerized medical care climate, as well as progressing research for powerful quiet security insurance and administrative consistency.

2. INTRODUCTION

The application of blockchain technology has grown in popularity in the past several years across several industries, including healthcare. A developing number of medical services associations are using blockchain innovation to safely, secretly, and interoperable oversee patient information. The healthcare industry is at a critical turning point when access to and efficiency from healthcare delivery are never conceivable due to the digitalization of patient data from Electronic Health Records (EHRs) to virtual consultations. It is more crucial than ever for healthcare companies to safeguard Protected Health Information (PHI) while they navigate the difficulties of digital transformation, given the rise in cyber threats and the complex legal landscape surrounding patient data protection.

Essential terms that serve as the foundation for comprehending the legal frameworks and legislation on patient data privacy are central to our conversation. Patient information digitalization is typified by Electronic Wellbeing Records, which offer a computerized substitute for traditional paper-based records (*Zhang, Xue, Liu*, 2019). Health Care Coverage Conveniences and Responsibility Act is a significant government rule in the US that contains guidelines for safeguarding delicate patient information. In like manner, the Overall Information Security Guideline (GDPR) is turning into a more relevant administrative structure for medical care administrations because of its expanded worldwide interconnectedness, particularly for firms that handle the information of EU people. This emphasizes the global nature of data privacy in healthcare.

This paper's thoughtfully crafted structure helps readers comprehend the many facets of healthcare data privacy. The first section of the article examines the situation of patient data privacy today, stressing the digital revolution in healthcare and its effects on data security. The article then makes cases for the need to have strong, multi-layered security mechanisms in place to properly protect patient data. To prepare for possible criticism, the report additionally addresses the difficulties and limitations that healthcare institutions may encounter when improving data security. This research emphasizes the need for a complete strategy to safeguard patient data through a thorough examination, highlighting the crucial role that organizational procedures, regulations, and technology play in accomplishing this objective.

3. PRIVACY ANALYSIS

Medical record privacy concerns working to safeguard individuals and their data by limiting third parties' illegal access to sensitive health information. Access control systems impose authorized

access to protected patient data in order to safeguard privacy. Protecting patient information while enabling the delivery of healthcare services is the aim of privacy in this situation. Privacy measures should thus be implemented to stop abusive and discriminatory activities, as well as the abuse and exploitation of data. For example, they can stop a health insurance company from refusing treatment or boosting a patient's healthcare expenditures, or they can stop an employer from discriminating against job candidates based on their likelihood of being sick or handicapped. Data sharing offers a few privacy risks that should be carefully considered and mitigated. The numerous challenges that the Internet of Things and online medical data sharing pose to the digitalization of healthcare are the main topic of this research review. The privacy analysis lists encryption, access control, and regulatory compliance as crucial precautions that are necessary to protect patient data in the healthcare industry. Millions of patient records are compromised every year by hackers targeting the healthcare industry, despite these attempts. Because of the important data they possess, healthcare organizations are prominent targets. As such, maintaining patient confidentiality and ensuring timely healthcare delivery require strong security measures to be prioritized. The report highlights the dual importance of secrecy for patient privacy and medical research, emphasizing how it protects private information communicated between patients and doctors while facilitating intricate research projects. The report also addresses how blockchain technology can provide safe, unhackable platforms for data interchange and storage, perhaps allaying privacy worries in the healthcare industry. To optimize blockchain's potential advantages in healthcare privacy protection, further study and innovation are required, as it recognizes obstacles including scalability problems and the requirement for specialist knowledge. Privacy analysis looks at how understanding information is kept secure in healthcare. It talks almost things like encryption, which turns information into mystery code that as it were certain individuals can

get it, and get to control, which limits who can see or alter the information. To create beyond any doubt understanding data remains private, there are rules like HIPAA, which sets benchmarks for how healthcare organizations ought to ensure information and rebuffs those who do not take after the rules.

But indeed, with these measures, there are still dangers. Cyberattacks, like computer infections or programmers, can break into healthcare systems and take delicate data. This could be a huge issue since patients ought to believe that their data will be kept secure when they visit a specialist. That's why confidentiality is so critical in healthcare. Patients got to feel comfortable sharing individual subtle elements approximately their wellbeing without stressing that it'll be shared without their consent. Innovation, like blockchain, is being looked at as a way to make strides in protection in healthcare. Blockchain is like an advanced record that records exchanges safely, making it harder for programmers to break in (*Javid, Haleen, Singh*, 2022). Be that as it may, there are still challenges to overcome, like making beyond any doubt diverse frameworks can work together easily.

In brief, the investigation appears that whereas healthcare organizations are working difficult to secure understanding information, there are still dangers that ought to be addressed. By utilizing innovation and following strict rules, ready to make beyond any doubt persistent data remains private and secure.

4. METHODOLOGY

Data will be shielded from breaches and vulnerabilities by the new technology known as blockchain. Solutions for the shortcomings of traditional healthcare data management systems are

provided by blockchain technology's immutability, transparency, and decentralization. The security and privacy of patient data in the healthcare sector are vital in the current digital era and need to be preserved in digital form, claim Azaria et al (*Azaria*, 2016). To do this, medical data monitoring using blockchain technology may be employed. Blockchain is a trustworthy source of truth since it is unchangeable and depends on public key cryptography for transaction security and transparency. Blockchain is essentially an unhackable, secure digital ledger that is used to log transactions. EHR security and privacy could be improved by using blockchain technology, for example. Blockchain based electronic health record systems could offer a secure, unhackable platform for patient data interchange and storage. The decentralized nature of blockchain technology allows it to prevent data breaches and guarantee data integrity. It can also guarantee that only those with permission can access the data by utilizing smart contracts and bitcoin payments. Another example is patient managed access, where patients choose who gets access to their data and can grant or revoke that access as needed. Blockchain based access control may also improve data privacy by letting patients grant or revoke access to their data whenever they choose and ensuring that only those with permission may access it. To maintain the integrity of patient data collected by these sensors, blockchain technology may enhance the security of protecting patient data.

5. BACKGROUND

Healthcare Information Management (HIM) started with the simple concept of recording patient care before Electronic Health Records (EHRs) became commonplace. Later on, healthcare IT services would be built upon it. When medical records were first created, doctors and patients could see all the information at their disposal to assess the course of therapy for illnesses, wounds,

and problems. When it came to storing records, computers in the healthcare sector were at first very limited. Representing a patient's medical and treatment history digitally, these records were called Electronic Medical Records (EMRs) and were limited to being stored at a single hospital. Software for electronic health records (EHRs), originally known as clinical information systems, represented a significant advancement in practice productivity and dependability. As the former made sure that PHI was truly secured, medical records and HIPAA law went hand in hand. Its rules apply to business partners, healthcare providers, clearinghouses, and health plans. A person's agreement is always required before sharing any sensitive information about them. Technology services for healthcare should adhere to these requirements. Blockchain adds an extra degree of anonymity to transactions by linking them to cryptographic addresses rather than actual identities when combined with other privacy enhancing technology. This pseudonymity increases patient confidentiality by lessening the possibility that private information may be connected to blockchain transactions (*Hannah, Xudong*, 2018). Although blockchain applications are expanding quickly, there is still a lack of general awareness regarding the technology itself and its potential. This is a barrier to the continued advancement and application of blockchain, which has the ability to drastically alter society and enhance the interchange of medical data, among other things. This technical solution primarily functions as a decentralized digital data storage system to immutably store digital data, enabling the safe sharing of created data, or meta-data, across users and networks. Blockchain is a list of records connected by cryptography. The data cannot be changed once it is recorded in a block without changing all subsequent blocks, which necessitates network majority consensus. This design makes data modification impossible. Blockchain, a decentralized ledger technology, enables independent actors to work together inside the ecosystem to guarantee transparency and time-stamped information recording, improving processing speed, revenue

creation, and security while lowering risk and expenses. By storing data in blocks and utilizing cryptographic keys, a distributed network, and a network servicing protocol, the blockchain's security is achieved. Metadata is recorded in a block once information (such as a transaction request) has been validated. Once this is done, it cannot be contested, removed, or changed without the networks and the people who produced the record's knowledge and consent. A block stays the same even after it is inserted into a chain with other blocks.

6. ARGUMENT

The main argument in favour of maintaining one's own privacy is the defence of one's own interests. On the other hand, the welfare of society is the main argument in favour of gathering personally identifiable health data for medical research. However, it’s crucial to emphasize that confidentiality is valuable to society as a whole because it enables complicated endeavours like investigations and public health initiatives to be drove out in a manner that uphold the worth of individuals. Simultaneously, medical study can be advantageous for people in that it can make fresh treatments, better evaluations, and methods of illness prevention and care delivery more accessible. Data obtained during a close relationship is protected by confidentiality. It deals with the problem of how to prevent outsiders from learning about data that is shared during those connections (*Yaqoob, Khan, Talib, Butt, Saleem, Nadeem*, 2019). For example, confidentiality forbids doctors from sharing data that the patient has discussed with them during a doctor-patient relationship. Confidentiality is violated when information obtained during a close relationship is unintentionally or unauthorisedly disclosed (*Gostin and Hodge*, 2002).

7. BENEFITS AND LIMITATIONS

7. 1. BENEFITS

Patients can have more control over who can access their data thanks to patient-controlled authentication provided by blockchain. Because it enables patients to access laws and make their medical data accessible, blockchain technology facilitates the shift to interoperability led by patients.

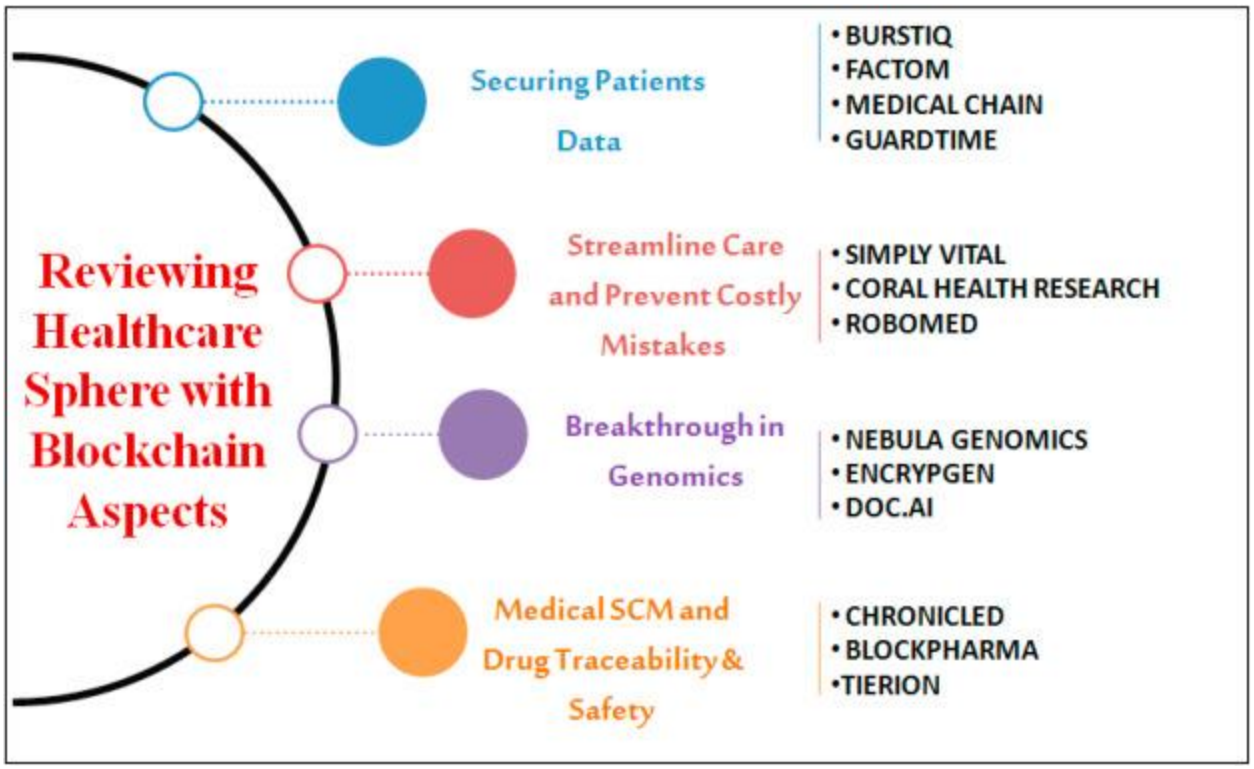

Figure ii: Blockchain implementation facilitators in the healthcare industry.

New patient data cards for doctors in other hospitals are created using blockchain technology. Most recently added material is repetitious and causes time waste, which is a serious health problem. Depending on where they are in the supply chain, each person may have varying rights or options. Furthermore, every block that had the medicine details would also have a hash linked to it from

another block. Moreover, the Blockchain framework's data transparency feature will aid in tracing the complete supply chain and ending the sale of fake medications. When a patient goes to a new clinic, a new medical card is created for them and deposited in a particular facility. Blockchain makes it easy to assemble issues with data processing.

More accountability and transparency in clinical trials could be possible with Blockchain technology. The medical service with the blocks made available to physicians and patients, and the medical history processed with consideration for patient concerns, blockchain technology offers tremendous record-keeping leverage (*Burniske, Vaughn, Cahana, Shelton*, 2016). In the healthcare industry, blockchain technology is particularly well suited for the supply chain and works well with pharmaceuticals. According to two studies, blockchain was also acknowledged as an authentication provider that allowed users to validate their access to health-related data services with just one ID. Through the use of timestamps recorded for every transaction, blockchain can help doctors track patient data more simply.

Blockchain increases openness in the healthcare sector when it comes to the sharing and keeping of patient data, medical records, details on the drug supply chain, and other vital data. Blockchain also gives patients the flexibility to manage who gets access to their data, guaranteeing accountability and transparency. By avoiding data breaches altogether, decentralized storage can do away with those expenses. Decentralized storage is an affordable alternative for storing healthcare data since it can also store vast amounts of data at a lower cost than standard storage. Blockchain technology is a solution to these issues because trust is a fundamental component of

it. Because of blockchain's immutability, patient data is kept safe and secure, alleviating worries and reestablishing confidence.

7. 2. LIMITATIONS

Even with blockchain's increased focus in the medical field, utilizing this technology for information sharing raises privacy and security concerns. Issues with scalability, data transmission latency, interconnections between various systems, data security, and secrecy are among the current limitations on the application of blockchain in healthcare.

One of the main drawbacks of blockchain technology has always been data immutability. It is evident that several systems, such as the financial and supply chain systems, gain from it. Every human being on the planet is entitled to privacy. That same person, however, won't be able to erase his trail from the system if he doesn't want it there if he uses a digital platform powered by blockchain technology.

To put it another way, you are unable to completely erase it, leaving your right to privacy intact. One of the issues with blockchain technology is the have to recruit several specialists in the sector, which is a drawback. They must also ensure that the management team is aware of the intricacies and outcomes of a business powered by blockchain technology, and they must teach current professionals in the use of blockchain (*Nakamoto*, 2008). Data is encrypted when kept on the blockchain, but if a patient's identity is connected to their encrypted data, there may still be a chance of unwanted access.

8. REVIEW AND IMPACTS

8.1. REVIEW

Decentralization is among blockchain technology's most essential features, and its two most important properties are immutability and censorship resistance. The user's level of trust in the information typically serves as a gauge for the caliber of medical data. Clean health records and databases further downstream could become more valuable. This Block technology helps in securely interchanging the data and storing patient privacy details and also it is a decentralized network that has the potential to completely transform the healthcare industry. Keeping medical data on the blockchain authentic is another difficulty. Errors or tampering with healthcare data could have a detrimental effect on patient care, so it is imperative that data be current and accurate (*Smith*, 2023). To maintain practicality and compliance with privacy rules, healthcare practitioners and organizations must carefully evaluate whether blockchain solutions are appropriate for their specific circumstances. In summary, the assessment provides valuable insights into the present status of blockchain technology's implementation in healthcare and identifies areas that need more investigation and advancement.

8.2. IMPACTS

Because hackers can access private data like Protected Health Information (PHI), cyberattacks directed at electronic health record systems pose a serious risk to patient confidentiality. Under HIPAA requirements, failing to protect patient records can result in significant fines and harm the organization's standing in the community.

Some of them include Cybercriminals, allegedly headquartered in China, used software weaknesses to obtain personal information such as names, birth dates, social security numbers,

phone numbers, and addresses, affecting four million patients in one instance of the Community Health Systems Data Breach in 2014. The training of staff members in identifying malware attempts, resolving common vulnerabilities used in these kinds of assaults, and keeping abreast of prospective software exploits via databases such as CVE are among the lessons learned from this intrusion.

Comparably, a ransomware assault on third-party vendor Blackbaud, which was responsible for storing Trinity Health's donor database, resulted in the May 2020 Trinity Health Data Breach, which affected around three million patients. Hackers were able to access some of the data despite defenses against the attack (*Haque, Hasan, Jiang*, 2020). In response, Trinity Health underlined the significance of putting third-party vendor monitoring solutions into place and stressed the hazards and unpredictability of complying with demands made by cyber criminals.

A hack on a third party file transfer network resulted in another compromise that affected about 600,000 patients and affected Trinity Health in 2021. This emphasizes the necessity of strong incident response strategies and increased awareness to lessen the effects of cyberattacks in the healthcare industry.

9. CONCLUSION

Blockchain technology has grown in importance as a technical trend for IS application creation. Therefore, gaining knowledge about landscapes is crucial to understanding better design processes. Critical obstacles to information dissemination and sharing exist in the healthcare industry. To make well-informed clinical choices, patients and providers must have access to a combination of secure data exchange tools. As previously said, digitizing medical data opens new possibilities for analyzing trends in medicine and assessing the standard of treatment. Additionally, as blockchain

technology continues to advance, it can provide several advantages for support services. In this research, we provide an automated approach to gathering pertinent published literature using a text mining algorithm, which effectively produced the desired results for carrying out the review study.

By emphasizing its possible uses in among peers information interchange, intelligent contracts, information preservation and swapping, and physician credentialing, blockchain technology is being applied to the healthcare sector. Furthermore, it is thought that Blockchain-based health reports can improve diagnosis precision, offer more information for choice of therapy, and be a more affordable option by using a database including health reports with distinctive information about patients. The need to highlight the blockchain's rapid adoption in the medical sector—which has been hampered by the issues is emphasized in the conclusion of the paper. This research project aims to provide a thorough understanding of the blockchain's application in the medical field. The results of the study offer potential study avenues that should stimulate creativity and advancements in the architecture of medical records, where blockchain technology can offer ways to distribute verified information.

10. REFERENCES

1. Gostin LO, Hodge JG. *Personal privacy and common goods: A framework for balancing under the national health information Privacy Rule*. Minnesota Law Review, 2002.
2. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: *Using blockchain for medical data access and permission management*, 2016.
3. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R.; Khan, S. *A review of Blockchain Technology applications for financial services*. BenchCouncil Trans. Benchmarks Stand. Eval. 2022, 2, 100073.
4. Zhang, R.; Xue, R.; Liu, L. *Security and privacy on blockchain. ACM Compute*. Surv. (CSUR) 2019,52, 1–34.
5. Hannah Chen, Xudong Huang. *Will blockchain technology transform healthcare and biomedical sciences?* EC pharmacology toxicol., 6.11 (2018).
6. Yaqoob, S.; Khan, M.M.; Talib, R.; Butt, A.D.; Saleem, S.; Arif, F.; Nadeem, A. *Use of blockchain in healthcare: A systematic literature review*. Int. J. Adv. Compute. Sci. Appl. 2019,10, 644–653.
7. Burniske, C.; Vaughn, E.; Cahana, A.; Shelton, J. *How Blockchain Technology Can Enhance Electronic Health Record Operability*; ArkInvest: New York, NY, USA, 2016
8. Nakamoto, S. Bitcoin: *A peer-to-peer electronic cash system. Decentralized Bus*. Rev. 2008, 21260.
9. Ul Haque, R.; Hasan, A.S.M.T.; Jiang, Q.; Qu, Q. *Privacy-preserving k-nearest neighbours training over blockchain-based encrypted health data*. Electronics 2020,9, 96.
10. Smith, J.A. *Blockchain Technology in Healthcare: A New Paradigm for Security and Privacy*. Journal of Medical Informatics, 2023.