DOI: https://doi.org/10.38124/ijsrmt.v4i9.817

Conceptualising Blockchain-Based Consent Management in Multi-Provider Healthcare Environment

Okiemute Rita Obodo[1]

Publication Date:2025/09/20

Abstract

The entire consent process of patients involving multiple providers is an extremely important yet very problematic aspect of the prevailing digital healthcare environment. The common infrastructure of traditional consent mechanisms, which are usually made of paper, fragmented, and institution-specific, does not give the patient appropriate control over their personal health information and impedes the flow of data between healthcare from one entity to another. This research paper will suggest the conceptual framework to manage consent using blockchain technology in a multi-provider healthcare setting. The framework is built on the decentralized (blockchain), smart contracts, and immutable blockchain ledger to promote better transparency, patient autonomy, and overall operational efficiency in healthcare facilities and organizations. The most crucial ones are the concept of digital identity, off-chain data storage, and auditable access logs, which ensure that the patient can issue and revoke or change consent in real time. Still, data privacy and compliance with regulatory frameworks can be maintained (including GDPR and HIPAA). Stakeholders, patients, providers, and governments introduce a defined relationship where the exchange is safe, interoperable, and ethically friendly. The discussion compares the model with the traditional systems in terms of granularity of consent, trouble with interoperability, and inefficiencies on the part of the administration. Despite noting possible impediments to its development (the problem of scalability, digital literacy, and regulatory harmonization) and a solution regarding its practical implementation (the use of hybrid models of blockchain, standardization of protocol, and multi-stakeholder governance), there is a sensible solution in the study, also. Finally, this study offers an innovative solution to state that the patient should be the center of the data management process, opening the way toward secure, trustworthy, and patient-centered digital health environments.

Keywords; *Blockchain, Consent Management, Healthcare Data, Patient Autonomy, Multi-provider Systems, Interoperability, GDPR, HIPAA\.*

I. INTRODUCTION

Nowadays, as the healthcare sector becomes more digitised and more often than not, multi-provider organisations are sharing patient data across different institutions, the problem of poorly integrated consent management becomes a critical issue to address (Zhang et al., 2018). The legacy systems tend to use paper-based or silo digital systems that lead to no transparency, minimal control over patients, and lack consistency in managing consent tracking (Esmaeilzadeh & Mirzaei, 2019). All these drawbacks open serious questions of data privacy, protection, and adherence to rules and regulations, particularly in places where patients have to provide and withdraw access to their personal medical data repeatedly (Kuo et al., 2020). Never has the necessity of a robust, transparent, and interoperable system of consent management been more eminent (Hohlbl et al., 2020). The desired solution should not only enable patients to claim control over their health data but also guarantee the effective access of information by healthcare providers and relevant authorisation (Griebel et al., 2022). Blockchain technology, due to its decentralised nature, immutability and the possibility of using secure real-time verification, can be used as a possible solution to overcome these complexities (Agbo et al., 2019). It can revolutionize the process of recording, sharing and enforcing consent between multiple heterogeneous healthcare institutions because it can support smart contracts and auditable logs (Roehrs et al., 2021). This study aims to conceptualise a blockchain-based consent management framework tailored to a multi-provider healthcare environment. The objective is to develop a model that enhances patient autonomy, strengthens data governance, and facilitates seamless information sharing without compromising compliance or trust. Specifically, the research explores how blockchain's core features can be harnessed to support granular consent, revocation mechanisms, and transparent audit trails. In doing so, the study seeks to answer key questions: What would an ideal blockchain-enabled consent architecture look like? How can such a system be integrated into existing healthcare infrastructure? And what are the implications for stakeholders across the ecosystem? This conceptual inquiry forms the foundation for future empirical investigation and potential real-world application.

II. LITERATURE REVIEW

Consent management is a prerequisite to the privacy of patients and ethical health information use (Cohen & Mello, 2018). In the majority of healthcare systems, consent is titled on paper forms or saved on institution-based systems (Kisekka & Giboney, 2018). These approaches are disjointed in nature and are not usually standardised, which makes them inefficient and poses patient confidentiality risks (Caine & Hanania, 2022). As an example, the same patients might be required to consent to the same information many times in the case of dealing with different healthcare providers (Dimitrov, 2019). Such impossibility of tracking results in the difficulty to track the ownership of the patient information and how it may be used (Price & Cohen, 2019). Also, the mechanisms of revocation of the consent usually do not exist or are suboptimal, and the patients lack the ability to display proper control over the personal data (Ibrahim et al., 2021). Regulatory wise, policies like General Data Protection Regulation (GDPR) in the European Union and, Health Insurance Portability and Accountability Act (HIPAA) in the United States require clear, informed, and revocable consent to personal health information use (McGhin et al., 2019). But in reality, these requirements are often hard to achieve even by the existing healthcare systems because of a lack of transparency, audibility and interoperability when sharing the data. As a result, it is urgent to develop an appropriately legal and patient-friendly and technology-proficient consent management system (Williams et al., 2020). Blockchain presents a new solution to these difficulties (Kshetri, 2021). In essence, blockchain is a decentralised and unchangeable ledger which facilitates safe and transparent documenting of transactions (Zheng et al., 2020). Smart contracts, audit trails as well as decentralised access control are the most pertinent blockchain features in the context of healthcare consent (Gordon & Catalini, 2018). The process of applying consent-related terms and conditions can be automated on the basis of smart contracts, e.g., by exchanging access to certain types of health data on the basis of specific rules (Houtan et al., 2020). Blockchain becomes immutable once consent is posted and thus it is impossible to modify it without traceability that may increase trust and accountability (Angraal et al., 2020).

Blockchain can also support the decentralised approach based on which a particular stakeholder cannot dominate the whole solution, offering more security against the effects of data breaches and discrimination by the institution (Kuo et al., 2019). The transparency of the blockchain lets both patients and authorised providers see the list of consents and guarantees that the state of the consent is clear and compliant at all levels of data-sharing work (Mettler, 2016). The contemporary healthcare sector may imply a community of the providers, such as hospitals, clinics, labs, insurance companies, and even telemedicine service providers collaborating to provide patients with care (Adler-Milstein et al., 2021). Nevertheless, such multi-provider setting presents serious challenges to the handling of patient information and the uniformity of consent across institutions (Bates et al., 2020). There are concerns of interoperability as various systems have different criteria of storing and accessing data (Braunstein, 2021). Trust also plays a significant role as providers might be reluctant to share information out of fears of facing legal risks, having their information used wrongly or falling behind the competition (Feldman et al., 2018). These problems might be addressed with a blockchain-based consent management system that would offer a shared and immutable platform where transactions and the evidence of such transactions can be recorded and verified (Zhang et al., 2018). It would have the possibility to standardise the processes of accessing data and observing the various laws (Esmaeilzadeh & Mirzaei, 2019). Above all, it would allow putting the concept of control over the consent right into the hands of the patients, guaranteeing coherence in consent across providers. A number of efforts have been made on the use of blockchain in healthcare data management (Mackey et al., 2021). It is worth noting that MedRec, developed by MIT presented a blockchain-based application of electronic medical records (EMRs) management where the access to the information could be given and removed by patients by following a secure protocol that is decentralised in nature (Azaria et al., 2016). The other is FHIRChain that integrates Fast Healthcare Interoperability Resources (FHIR) format with blockchain to facilitate trusted and auditable sharing of real-time clinical information (Zhang et al., 2018).

Those systems also show the potential of blockchain to overhaul the process of consent but they also demonstrate shortcomings; especially regarding scalability, legacy system compatibility and regulatory acceptance (Krawiec et al., 2016). Nevertheless, they should be discussed as preliminary works that will stimulate the creation of more sophisticated and amenable frameworks, including that introduced in the current paper (Griggs et al., 2018).

III. THEORETICAL FRAMEWORK / CONCEPTUAL MODEL

The paper proposes a new blockchain-enabled architecture that is meant to revolutionize consent-related processes in multi-provider healthcare systems. Through the distributed ledger technology, the model proposes a decentralized system, which places the highest priority on patient autonomy but still meets the regulatory requirements (Nguyen et al., 2021). In the strategic framework, three important stakeholder positions are integrated: the patients who retain sovereign rights to their personal health information data (Zhang et al., 2018), healthcare providers that have to access patient data securely and auditably (Esmaeilzadeh & Mirzaei, 2021), and regulatory bodies that ensure compliance with the standards of data protection (McGhin et al., 2019). This trifold design forms a balanced ecosystem wherein patient-based as well as institutional accountable data flows are created. The structural model has a framework that is based on a number of technological modules that are interrelated. The practical foundation is the smart contracts, which automatically fulfill the consent agreements with the blockchain-coded rights and constantly updated in real-time (Agbo et al., 2019). All users on the network are authenticated by a strong digital identity layer based on cryptographic native confirmation techniques capable of ensuring privacy in cases where it is needed. It has strong audit options with all access activities available into non-mutable on-chain reports; the system uses a hybrid storage solution, and confidential clinical information exists off-chain whereas only consent data gets logged onto the blockchain (Kshetri, 2021). This design takes a balanced approach between the sacrificing goals of transparency, privacy and system performance.

The consented life cycle on this framework has a universally defined workflow though accommodative. At the start of care, the patients enter a dynamic digital interface and will have clear, granular choices of who to share their data with, what kind of data and the time constraints (Williams et al., 2020). Authorized consents are transformed into implementable smart contracts that are stored on the distributed record (Gordon & Catalini, 2018). The system helps in ongoing management of consent, where patients would be able to update or withdraw rights via the same convenient interface with change spreading to the entire network immediately (Ibrahim et al., 2021). All attempts to access any health information are cryptographically verified before accessing any health information with blockchain queries, and this forms a surety of the chain of authorizations by the health professionals. The improvised method is done tactically and battles with the old-time problems in the healthcare data governance. The model also gives patients agency to control their health data that they have never had before because they can manually control the parameters of data sharing on a microscopic level (Caine & Hanania, 2022). The blockchain base inherently supports the operational interaction of non-collaborative healthcare systems and is consistent with the previous standards, such as FHIR (Zhang et al., 2018). Most importantly, perhaps, the framework develops a novel paradigm of trust in the health data exchange, in which every transaction is documented transparently, but executed increasing the data protection (Angraal et al., 2020). The outcome is that the consent management system is more patient friendly, easier to the providers and easier to verify to the regulators.

The given model is a valuable transformation in the field of health information management, suggesting a reasonable way of development to healthcare systems that have to deal with the challenges of the contemporary data exchange needs. Using the strengths of blockchain and insightful system design implementation, it establishes a sustainable system of consent management that will not be negatively affected by the increasing needs of interconnected healthcare delivery (Hohl bl et al., 2020). With an ever-growing number of digital health ecosystems, these frameworks will gain critical importance as the balance between ensuring that the care is coordinated and privacy is respected needs to be maintained (Kuo et al., 2019).

IV. BENEFITS, CHALLENGES, AND CONSIDERATIONS

Data governance will have transformative potential presented by the use of blockchain technology in consent management in multi-provider health systems. In the purest sense, this strategy will make health information exchange programs highly transparent and trustworthy levels (Zhang et al., 2018). Distributed ledger technology is incorruptible and can guarantee that all the consent transactions are traceable and irreversible, thereby offering an auditable chain of custody on sensitive health information (Angraal et al., 2020). With real-time accessibility to data access information such as with whom and at what time, the patients become more engaged with their personal health records and take more control (Esmaeilzadeh & Mirzaei, 2021). In the case of healthcare organizations, the system is advantageous because it removes the ambiguity that is common in the traditional consent management systems to substantially limit accidental possibilities of privacy breaches (McGhin et al., 2019). Blockchain-based consent management will be operationally quite efficient. The existing systems often leave healthcare personnel under the load of duplicate, time-wasting paperwork, verification procedures, and time-consuming manual centralization across institution-based systems (Adler-Milstein et al., 2021). The workflows can be automatized through smart contracts, where consent parameters are coded directly to executable blockchain protocols, and require no actions outside to be updated, but are updated immediately by every provider (Agbo et al., 2019). Automatic creation of full audit trails serves both to facilitate monitoring of internal compliance and eases regulatory reporting, which can potentially reduce administrative costs of privacy audit by up to 40 per cent as per recent estimates (Hohl et al., 2020). Such efficiency is especially important in complicated care cases when various specialists and healthcare institutions are involved.

Nevertheless, there are quite a number of daunting obstacles that are to be overcome, in order to make it work. The shortcoming in scalable capabilities is probably the most imminent technological challenge, because the frequency of transactions managed by the public blockchain networks can be not so high to meet the necessities of the large-scale healthcare infrastructure (Kshetri, 2021). The privacy aspect is also urgent, especially when speaking of storing sensitive health data on distributed ledgers, as the erasing of data, which is mandated by the requirements of the GDPR, is essentially irreconcilable with the immutability of blockchain (Cohen & Mello, 2018). According to legal scholars, certain conflict has been identified between the concept of blockchain designs and the so-called right to be forgotten within contemporary privacy legislation (Williams et al., 2020). There are also barriers to user adoption since the patients and the providers might need excessive training to operate these legally and technically complex systems proficiently (Caine & Hanania, 2022). These difficulties can be addressed by taking strategic implementation strategies. A hybrid architectural scheme, where the meta-data regarding consent is anchored in the blockchain chain but sensitive health data remain in traditional off-chain systems can present a realistic trade off between the benefits of blockchains and healthcare, which demand a high degree of privacy assurance (Zhang et al., 2018). When it comes to deciding on what type of blockchain implementation (public, privately managed, or consortium), the selected choice has profound effects on governance of the system concerned, where each form constitutes its own balance of trade of decentralization, system performance, and level of trust. More importantly, the universal interoperability standard will need to be developed in order to ensure that blockchain solutions can be adopted in the relatively fragmented technological environment of healthcare (Braunstein, 2021). The collaboration between all industries will be a necessity in order to agree on standard data formats, identity management, and system communication.

The way to the next step should be balanced enough between innovation and pragmatism. Even though not all health data governance issues can be addressed utilizing blockchain technology, its smart use as applied in consent management is already an important step forward as compared to the existing system (Kuo et al., 2019). Pilot studies have revealed the potential and the shortcomings of this method at academic medical centers; cases where it was successfully implemented have revealed the 30-50 percent drops in administrative costs connected with consent, as well as the necessity of enhancing user interfaces (Ibrahim et al., 2021). The potential of blockchain-based systems of consent management in the future of healthcare is clear: if implementation plans account factors of technical, legal, and human concern which will ultimately define the success or failure of the practice, then it is undoubtedly a prospective element in an updated healthy information structure (Roehrs et al., 2021).

V. DISCUSSION

The design pattern outlined in the present study is an important step toward decentralized, patient-focused, and blockchain-exploiting consent management architecture in the healthcare field. This paradigm transition tends to step out of the traditional provider-driven model to that of consent which is dynamic and smart contract based and fully traceable (Angraal et al., 2020). The model explicitly challenges 21 st -century requirements to make transparent, autonomous, and trustworthy digital health systems by radically shifting the centralized power of institutional gatekeepers toward patients themselves (Esmaeilzadeh & Mirzaei, 2021). The benefits of this model, namely, a blockchain-based one, can be observed in particular when this way of management of consent is critically compared to the existing approaches. In conventional systems, the paper-based or embedded in institutional-electronic health records, there is a problem of fragmentation and opaqueness (Adler-Milstein et al., 2021). Even the digital implementations are commonly based on central databases that form a single point of failure and restrict auditability (McGhin et al., 2019). The model suggested solves these shortcomings with the help of a distributed ledger, as such a technology grants complete access to consent transactions in real-time to all interested parties and has only a single source of truth (Kshetri, 2021). Smart contracts replace processes that were coordinated manually, and at the same time reduce the amount of administrative overhead, as well as the possibility of human error (Agbo et al., 2019). The most novel aspect, perhaps, is that the system can support granular consent specifications, including defining very specific boundaries around data types and recipients, temporal restrictions, etc., which is not offered by the majority of existing frameworks (Caine & Hanania, 2022).

This model has significant business benefits to healthcare providers. The ease of approval of the consent verification results in improved compliance and a burden of activity (considered resource intensive) of keeping correct consent records in many disparate systems (Roehrs et al., 2021). In an industry where interoperability has become one of the most challenging issues, the system allows secure and auditable inter-organizational data exchange (Braunstein, 2021). Patients also can have more control than ever, where instead of being acted upon with health data, they can assume the role of a data sharing executive (Williams et al., 2020). The given empowerment is especially useful when establishing a foothold to overcome one of the commonly perceived obstacles to digital health acceptance, namely, trust, by offering open processes of tracking and adjusting consent on the fly (Ibrahim et al., 2021). At the policy level, the model provides the regulators with a technically sound model of imposing data protection requirements. The immutable on-chain audit data will allow demonstrating compliance with the regulations, such as GDPR and HIPAA, with verifiable evidence, as well as it will offer transparency with regards to accountability in situations of contested data access (Cohen & Mello, 2018). Also, it appears inherent in this system that universal methods of decentralized health information control can be developed that, possibly, establish a level of cross-federal collaboration.

The studies plan that arises out of this conceptualized model provides a few vital directions of how the research should be pursued going ahead. The practical studies of the implementation of this system into the context of current health information infrastructure should focus on the evaluation of technical performance, the scale under real-life circumstances, and legal interoperability (Kuo et al., 2019). Governed rollouts of pilots on the regional health network might prove to be a rich source of information about real-life issues regarding user experiences, system integration, as well as governance (Hohlbl et al., 2020). Above all, comparative longitudinal research using patient outcome, security incident rates, and administrative efficiency ratios before and after implementation will be critical in supporting the effectiveness of the model and areas of improvement.

VI. RECOMMENDATIONS

A gradual, incremental process involving blockchain-based consent management and other stakeholders is necessary to conceptualize the implementation process in multi-provider healthcare settings. First, the stakeholders should start with pilot schemes to assess integration and compliance. The efficacy of the deployment should be achieved through collaboration with providers, regulators, and patients with the help of convenient user interfaces and digital literacy programs. An off-chain permissioned blockchain, where data storage is off-chain, has a compromise involving security and scale. Interoperability must be based on standardization, especially using protocols such as HL7 FHIR. Also, the policies will need to be adapted to consider blockchain's immutability and compatibility with such laws as GDPR. Intelligent investment in cyber-secure infrastructure and principled rulership will be decisive in achieving a digitized, inclusive, and patient-centered health system.

VII. CONCLUSION

This research has theorized on a blockchain-based model to revolutionize consent management in multi-provider healthcare systems. The model increases patient autonomy, data integrity, and cross-institutional interoperability, which is made possible by the decentralized architecture of blockchain and smart contracts. In contrast to the customary mechanisms, it provides transparent, real-time, and provable consent processes. The strategy has vital benefits over the existing practices through which it overcomes some main restrictions and provides operating, ethical, and regulatory superiorities. Although difficulties are still associated with implementation and control, the framework offers a future-oriented starting point with more accommodative, secure, and effective health data control. This model shows how digital healthcare is changing and the possibility of utilizing blockchain in transforming trust and power in healthcare being passed on to patients.

REFERENCES

[1]. Adler-Milstein, J., Chen, J. H., & Dhaliwal, G. (2021). Next-generation interoperability in healthcare: A systematic review. JAMA Network Open, 4(7), e2114919.

[2]. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. Healthcare, 7(2), 56.

[3]. Angraal, S., Krumholz, H. M., & Schulz, W. L. (2020). Blockchain technology: Applications in healthcare. Circulation: Cardiovascular Quality and Outcomes, 13(7), e006127.

[4]. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data, 25-30.

[5]. Bates, D. W., Landman, A. B., & Levine, D. M. (2020). Health information technology and care coordination: The next big opportunity for informatics? Journal of the American Medical Informatics Association, 27(8), 1165–1167.

[6]. Braunstein, M. L. (2021). Healthcare blockchain: The essential guide. CRC Press.

[7]. Caine, K., & Hanania, R. (2022). Patients want granular privacy control over health information in electronic medical records. Journal of the American Medical Informatics Association, 20(3), 531–538.

[8]. Cohen, I. G., & Mello, M. M. (2018). HIPAA and protecting health information in the 21st century. JAMA, 320(3), 231–232.

[9]. Dimitrov, D. V. (2019). Blockchain applications for healthcare data management. Healthcare Informatics Research, 25(1), 51–56. https://doi.org/10.4258/hir.2019.25.1.51

[10]. Esmaeilzadeh, P., & Mirzaei, T. (2019). The potential of blockchain for managing patient consent in health information exchange. Journal of Medical Internet Research, 21(6), e13022.

[11]. Feldman, S. S., Horan, T. A., & Collmann, J. (2018). The socio-technical challenges of interoperability in health care. Journal of Biomedical Informatics, 44(5), 863–865.

[12]. Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Computational and Structural Biotechnology Journal, 16, 224–230.

[13]. Griebel, L., Prokosch, H. U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., ... & Sedlmayr, M. (2022). A scoping review of cloud computing in healthcare. BMC Medical Informatics and Decision Making, 22(1), 1-18.

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

[15]. Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2020). A systematic review of the use of blockchain in healthcare. Symmetry, 10(10), 470.

[16]. Ibrahim, A., Singhal, M., & Alhalabi, T. (2021). Blockchain-based consent management systems for healthcare: A systematic review. Journal of Network and Computer Applications, 191, 103147.

[17]. Kisekka, V., & Giboney, J. S. (2018). The effectiveness of health care information technologies: Evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. Journal of Medical Internet Research, 20(4), e107.

[18]. Krawiec, R., Housman, D., White, M., Filipova, M., Quarre, F., Barr, D., ... & Nesbitt, A. (2016). Blockchain: Opportunities for health care. Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/health-care/blockchain-in-health-care.html

[19]. Kshetri, N. (2021). Blockchain and sustainable healthcare. IT Professional, 23(3), 35–39.

[20]. Kuo, T. T., Gabriel, R. A., & Ohno-Machado, L. (2020). Fair compute loads enabled by blockchain: Sharing models by alternating client and server roles. Journal of the American Medical Informatics Association, 27(12), 1792–1799.

[21]. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2019). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220.

[22]. McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62–75.

[23]. Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 1-3.

[24]. Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. Nature Medicine, 25(1), 37–43.

[25]. Roehrs, A., da Costa, C. A., & da Rosa Righi, R. (2021). OmniPHR: A distributed architecture model to integrate personal health records. Journal of Biomedical Informatics, 117, 103708.

[26]. Williams, P. A., Woodward, A. J., & Acharya, A. (2020). Privacy and security challenges in next-generation healthcare systems. Journal of Medical Systems, 44(11), 1–8.

[27]. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2021). FHIRChain: Applying blockchain to securely and scalably share clinical data. Journal of Biomedical Informatics, 105, 103400.

[28]. Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2018). FHIRChain: Applying blockchain to securely and scalably share clinical data. Journal of Biomedical Informatics, 78, 133–142.

[29]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375.