[1] Lenigrace L. Mecias

[2] Thelma D. Palaoag

Establishing Robust Data Sharing Through a Blockchain-Driven Standardization Framework in Local Community Healthcare System

Abstract: - The healthcare industry's digitalization has sparked innovation and improved various aspects of the services. Community hospitals in Pangasinan still use conventional paper-based methods for managing patients' health records. However, the healthcare information system is still in a traditional structured excel platform and lacking of communication among healthcare providers. This study aims to design a blockchain-driven standardization framework to establish robust data sharing and increase the confidentiality and security of stakeholders in using the healthcare system. In gathering data, a focus group was organized to give a valuable perspective on the present state of the healthcare system through conducting an online survey, seven respondents are direct users of the healthcare system. The study adopted the IS4H assessment maturity tool concerning data management and information technology in identifying the gaps and challenges in the existing healthcare system. A comprehensive review of related literature regarding the usability of access control models in the study and the potential of blockchain technology in the healthcare system is also essential. Blockchain technology provides features that enhance the accessibility and immutability of the healthcare system and to the stakeholders. The research underscores the paramount importance of integrating blockchain, access control, and security measures to safeguard privacy in the system. The implication of the integration of blockchain is seamless, secure, and patient-centric which has a great potential to contribute to improving the digitalization of healthcare quality of services in the healthcare system.

Keywords: Access Control, Blockchain, Decentralized, Healthcare Information System.

I. INTRODUCTION

Today digitalization in various fields is now increasing the need to innovate and revolutionize technologies. Integrating these technologies has been explored, undergoing significant advancements and transformations, including the notable development of blockchain technology. It is crucial for local community hospitals to continually enhance their services, with a particular focus on patients' health records.

Cutting-edge technologies like blockchain innovation play a significant role in fulfilling the requirements of various sectors, including education, business, and healthcare. Blockchain was created by Satoshi Nakamoto, and first introduced the Bitcoin transaction in the internet. As technology continues to revolutionize, the role and influence of blockchain are rapidly growing. Dagher, 2018 proposed the use of blockchain technology, specifically a framework in the healthcare sector called Ancile that aims to strike a balance between the confidentiality of electronic health records and their ease of access. [1]. Ancile utilizes an Ethereum blockchain and smart contracts to guarantee the security, integrity, and streamlined accessibility of health records for patients, healthcare providers, and external entities. Blockchain protects data and concluded in the study by Ghosh [2], that challenges like patient engagement will be more effective if they can access the platform through cryptography capabilities to provide more secure irreversible, and immutable data access [2]. Data exchange mechanisms in different healthcare providers are also possible in blockchain, it reduces costs and is transparent to all stakeholders. The main purpose of blockchain is to make data accessible, and immutable and promote security and privacy.

Local community hospitals in the province of Pangasinan are also in need of a system to provide potential technological solutions to help the community acquire a digitalized healthcare system for quality of services. The slow processing of the healthcare system also affects the likelihood of patients going to the hospitals [3]. Furthermore, The Department of Health (DOH) also listed the subsequent concerns for future advancements in eHealth, acknowledging its significant role during the pandemic. However, there are certain insufficiencies in these system components, such as the absence of data sharing between electronic medical records and different data formats of health information systems, which indicates not sufficient support systems to handle these issues [4].

They aim to make the healthcare system accessible and available to people in the community to provide quality healthcare services [5]. Communication among healthcare providers is significant however, services for patients

[1, 2] College of Information Technology and Computer Science, University of the Cordilleras, Baguio City
Email: [1] leni1920mecias@gmail.com, [2] tdpalaoag@uc-bcf.edu.ph

suffer the consequences due to delays in processing medical records and referrals due to the unavailability of communication lines which was mentioned by Gilbert in his article [3].

Furthermore, this suggests that not every hospital has embraced digital technologies for patients' medical records or healthcare information systems. Only one-third of the hospitals have adopted electronic medical records [4]. Therefore, interoperability is difficult for local community hospitals to deliver. When patients seek medical care services, their information is manually recorded on physical documents such as medical charts and forms. This traditional approach has resulted in several issues, like it leads as delays in accessing critical patient information due to the need for manual searching of records [6]. Moreover, relying on paper-based data sharing introduces risks related to errors, security, and privacy breaches when accessing patients' data [7] [3]. Additionally, the physical storage of records poses challenges, including limited space and difficulties in managing and organizing the ever-increasing volume of patient data [8]. As a result, healthcare providers find themselves burdened with the growing task of maintaining and managing paper-based records [7].

Furthermore, the security of stakeholders and accessibility of resources like patient records are also significant but limited in the sharing of data across healthcare providers. By becoming resilient and having a sustainable healthcare system, the government upholds the capacity to adapt and transform not only in the service delivery but also in the healthcare system and IT infrastructure [5].

Digitalization of systems helps the organization improve their functions as well as their services. Blockchain is an integral solution due to its features like immutability, tamper-proof, and traceability and it is a decentralized system in a distributed network [9].

In the context of unauthorized access to patient data, as discussed in their paper [10], which they proposed a blockchain framework that addresses decentralized data access and sharing challenges. This framework adopts a public key infrastructure model that includes signature cryptography algorithms, such as asymmetric cryptography algorithms. [11].

Additionally, advanced cryptographic methods are employed to enhance the overall security of the system. Author Wang mentioned that the application of blockchain public ledger is in the form of distributed constant protocol and can create cryptography, a peer-to-peer network, smart contracts, and decentralized [12][7][13]. Data sharing and distribution address the failures commonly encountered in centralized systems, such as security and privacy concerns.

All healthcare providers have their perspectives way to adapting to digitalization. The most essential issue in the medical system is the sharing of patient’s clinical data. Likewise, in KSA [14] [11] [12] they pointed out that data sharing within their hospital is a major obstacle due to lack of confidence and trust among healthcare providers [12][11][14]. In their work, authors A. R. Lee, M. G. Kim, and I. K. Kim introduced SHARECHAIN, a system that addresses reliability and interoperability concerns through two key features [15]. First, it enhances reliability by leveraging blockchain registry data integrity, and it establishes a consortium blockchain network for secure data sharing exclusively among authenticated institutions. [15] [16] [17]. The importance of role-based access control is enforcing access to objects and system functions is determined by the subject's predefined role or who is requesting the said resources while attribute-based access control specified organizational attributes like identity, functions, or authority to add, or delete, environmental attributes refer to the time or location and resource attributes like records or documents.

The objectives of the study are to identify the gaps and challenges in the existing healthcare system in MCH and to recognize the advantages and usability of access control models to enhance security and privacy which will be integrated into the proposed system. And able to design a conceptual framework that establishes robust data sharing through a block-driven standardization approach.

II. METHODOLOGY

This section discussed the methods in gathering of data to processing techniques.

At the beginning of the research, data collection was carried out via a well-organized focus group, which yielded valuable insights into the current state of the healthcare system through conducting a survey on the healthcare information system utilizing the Information Systems for Health Maturity Assessment Tool (IS4H-MM) in relevant to the data management with information system[18], governance and digital transformation in finding the current gaps and challenges in the existing healthcare system in Manaoag Community Hospital (MCH). A comprehensive review of related works in determining the usability of access control models. Components of Blockchain-driven standardization framework (BDSF) and integrating the decentralized personal identification into the proposed healthcare system are significant in the data sharing scheme to enhance security and privacy of users.

A brief description about the current state of healthcare system in Manaoag Community Hospital (MCH) and surfaced by cross-case analysis for the results from the conducted online survey using the IS4H-MM assessment tool in identifying the gaps and challenges in the healthcare system. A comparative analysis in combining the access control models in mitigating data sharing on its security and privacy issues.

Participants in the focus group includes registered nurse, record staff, admin aide, clerk, vocational graduate and admin and six (6) employees of Manaoag Community Hospital and one (1) in Pangasinan provincial hospital, there are seven (7) respondents who have responded the online survey produced via Google Forms and 130 questions was provided to the respondents.

III. RESULTS AND DISCUSSION

A. *Brief Description of Existing Healthcare System*

The current healthcare system in local community hospital (MCH) was using a structured Excel format platform in data collection for patient's records. The admin collects data sources through paper-based methods like tally sheets and paper forms and being encoded and stored in the database available in their office. Traditional process in collecting of data from their patient through charts and forms and properly kept in their medical records' room. The key data sources being collected are from hospital statistics and vital indices in real time manner. The dissemination of health records for retrieval and borrowing of charts to the internal entities or authorized personnel was also monitored through the use of logbook and standard procedures based from the hospital's policy. Accessing of medical records is prohibited but not limited to the authorized personnel. Communication like referral system is through phone lines to other healthcare providers. The health data standards that have been embraced, including classification systems, data standards, and medical terminologies. The healthcare has sufficient IT staff in managing their healthcare information system. In Table I, the subsequent findings were listed and surfaced by cross-case analysis for each domain such as DMIT, MAGO and IT Innovation Infrastructure and Architecture and highlighted the indicators from the conducted survey using IS4H tool. It is helpful tool and it is capable in identifying the gaps and challenges from the existing healthcare system, where each domain pointed out the identified issues and considered to be the indicators that need solutions in improving the healthcare system as shown in Table I.

Table I. Identified Gaps and Challenges

IS4H-MM DOMAINS	INDICATORS
DATA MANAGEMENT AND INFORMATION TECHNOLOGY	• The organization produces information products using a mix of structured and manual formats, but lacks the necessary equipment for maintaining and updating healthcare-related databases and maps. Moreover, there is no integration of interconnected and compatible health information systems, and data exchange services, directory services, and software development guidelines have not been implemented.
MANAGEMENT AND GOVERNANCE	• Healthcare system services/functions are acknowledged but not yet in operation. • Public health communication is responsive to national priorities, like managing outbreaks and disasters. • Data and information flow seamlessly between central, local, and public entities, with a feedback-driven approach. • Engagement with civil society and the public includes participation in governance bodies and utilizing social networks and platforms such as Facebook, Messenger, and Instagram.
IT INNOVATION INFRASTRUCTURE AND ARCHITECTURE	• Absence of an established data analysis procedure. • Healthcare operations are primarily manual. • Critical datasets for disaster response are missing. • Lack of a data backup strategy for supporting essential health system functions and disaster response.

In the realm of data management and IT, there is a deficiency in the required equipment for the upkeep and updating of healthcare records, which hampers data collection. Communication within MAGO primarily relies on social media, lacking a suitable platform for effective communication. Additionally, due to fragmented systems among healthcare providers, there are challenges in accessing health records, as data analysis and data sharing are hindered by inadequate storage capacity.

B. ACCESS CONTROL MODELS

The presented table (see Table II) are the different approaches in using access control models in the system. The comprehensive analysis to support in the adapting of attribute-based and role-based access control models from different valuable references. After analyzing the relevant literature, it becomes evident that various sources have incorporated distinct access control models into their research. These models have been applied for diverse functions and objectives, all with the aim of enhancing user authentication and authorization within the healthcare system to bolster data security and privacy. Nevertheless, in this research, the suggested approach integrates both healthcare system models, potentially enhancing user adoption of the proposed healthcare system and improving the quality of healthcare services they receive.

Table II. Comprehensive Analysis of Access Control Models

ABAC	APPROACH	RBAC	APPROACH
✓	To ensure the safe transmission of symmetric keys and data information. [13].	✓	Authorized Doctor can access patients' health record through account of patient and deployed addresses [12].
✓	Privileges to users through attributes [19]	✓	Role-based is significant in this study, only authorized doctors and patients can access their data [2].
✓	Ensure that the data can only be accessed by the user with proper attributes [9].	✓	Grants request to only authorized user [22].
✓	Implemented Abac for user identification or restricting trusted users or nodes responsible for managing sensitive data [20].	✓	Multiparty patient verification [6]
✓	Gradually increasing its users and able to limit for security and surveillance breaches in patients' privacy [21].	✓	Decoupling of authorization to access the images [12]

C. System Architecture: Decentralized Personal Identification (DPID)

The workflow of the proposed system and including the components to establish a robust data sharing scheme. The system architecture (see Fig 1) describes the following components to be integrated in the proposed system such as the user registration, employing the decentralized personal identification (DPID), security and privacy, smart contract, data storage and the data sharing scheme.

D. *Users' Registration*

Initially the users (admin, doctor and patients) should have acquired their accounts or public keys/private keys in Ethereum DApp (Metamask). The admin has the full access in the system managing and adding of users in the system. Patient will register her/his profile data into the application and required to add her/his personal identification card (PhilSYS ID) as a credential in DPID.

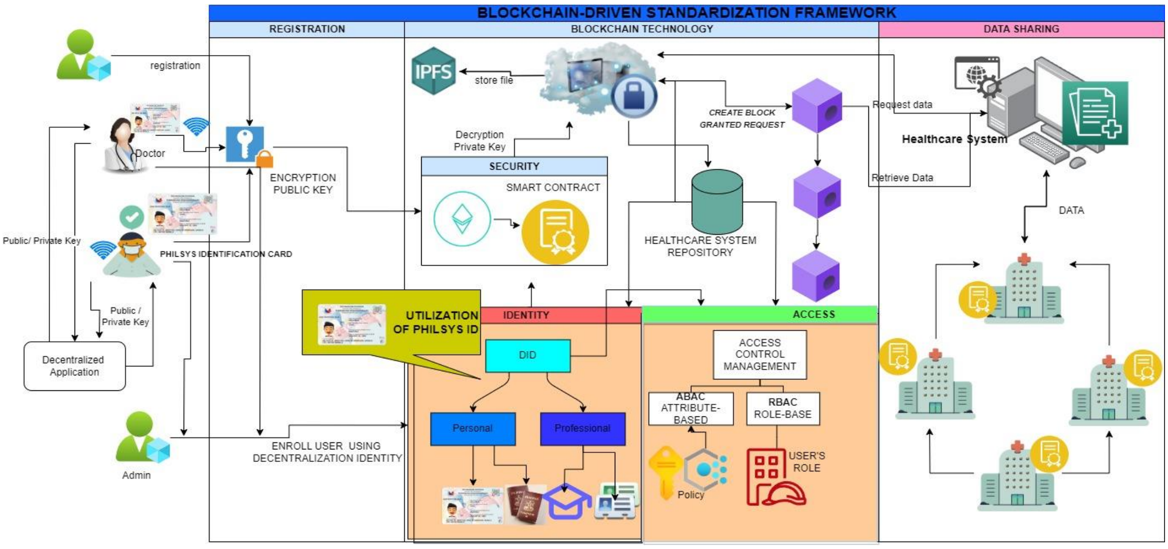

Fig. 1. Proposed Blockchain-driven Standardization Framework

This research combines the concept of the two access models ABAC and RBAC which are employed in the study to enhance security, authentication, and authorization capabilities. Adapting the access control management from NIST framework for Information Systems and organizations about the security of information and the organization, the role-based access control (RBAC)-AC-3(7) and attribute-based access control (ABAC)-AC-3(13) are applicable in the proposed system. The automatic revocation or authorize access in an individual's bringing user organized based on their roles. ABAC will provide access based on the resource access policy, and adapting these models is crucial to enhance the security and privacy for healthcare providers. In the proposed system, users' attributes like name and identification numbers are significant in accessing the system and roles like doctor and patients are the main users and can access the system. Their role must be well defined in the system for authentication and accessibility using their account in the system during the enrollment or registration. Doctor can add users in the system and as well as patients, using their public key account. Access control will be based on the healthcare policy and guidelines.

E. *Employing Users' DPID*

In a decentralized healthcare system, the traditional forms of personal identification (e.g., usernames, passwords, or social security numbers) might not be suitable due to security and privacy concerns. Adding security measures for the users is significant to reduce identity fraud and other untrusted cases in relevant to users' identity. Decentralized identification ensures that users have control over their identity and can grant or revoke access to their data as needed. The decentralized personal identification card (DPID) using ids such as (PhilSYS ID card) will be utilized into the system; it serves as the universal identifier (UID) of user for authentication and authorization as the main requirement in the access control management for the security and privacy of stakeholders with regards to the data sharing process in the healthcare system. Professional Identification can also be used as additional credentials. Furthermore, these access control models protect data, as well as devices and cloud services from unauthorized users. The Sybil attack represents a highly perilous threat within the blockchain ecosystem, as it directly undermines the system's integrity by creating counterfeit identities within the peer-to-peer network. To protect the system and users, through identity validation using the DPID can prevent this attack in the system.

F. *Security and Privacy*

Blockchain is a decentralized system that stores data that is immutable and tamper-proof. Additionally, data protection is essential to users also to healthcare professionals for ethical reasons. To protect the data, Rivest-Shamir-Adleman (RSA) is an asymmetric encryption algorithm that is widely used for secure data transmission and digital signatures. For data integrity, SHA-256 was used in the asymmetric algorithm or public key cryptography which protects the data where the public key is used for the encryption of data then only the private key will decrypt the data both keys should be owned by the same user.

G. Using Smart Contract

Smart contracts are automatic agreements coded on the blockchain that systematize and administer predefined rules and conditions. The creativity of smart contract on patients record and this paper also adapted their concept where smart contracts have the following functions such as assign roles, accept and cancel transaction approach [7]. This paper, smart contract with access control management with roles for admin, patient, and doctor, and attributes like name, address, and decentralized personal identification number (DPID) are merged in the automated aggreement. In this contract, a User struct that stores the role and attributes for each user (name, address,age, ID) where data matches from the DPID stored in the reposiroty (see Fig 2). The admin is set during contract deployment, and only the admin can register and confirm new users for validation. Patients and doctors can update their attributes. The contract also includes modifiers to limit access based on the user's role.

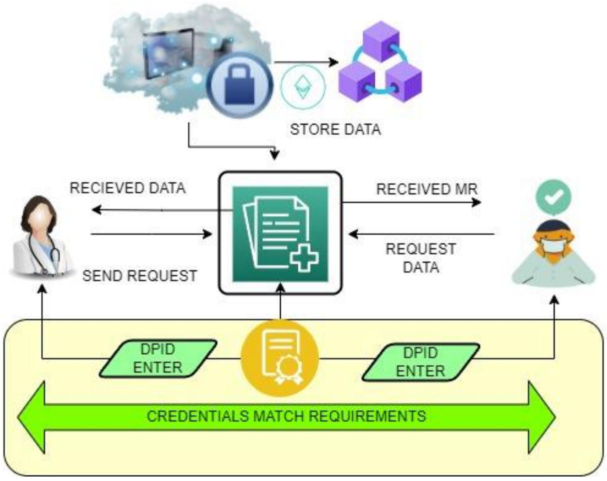

Fig. 2. DPIP for Data Sharing Mechanism

H. Data Storage

Blockchain operates distributed ledger technology (DLT), serving as a decentralized database that records information regarding transactions among different participants. Transactions are arranged in chronological order and stored as blocks within the ledger. IPFS enables healthcare system to store medical data in a distributed and decentralized system. Instead of relying on a central server, patient records and other medical information can be distributed across a network of nodes, making it more resilient to failures and reducing the risk in data breaches. By utilizing IPFS and blockchain, healthcare systems can ensure the integrity and immutability of medical data. IPFS hashes the data, and this hash is then recorded on the blockchain. Any change to the data would result in a different hash, making it immediately evident that the data has been tampered with. These features manage patient consent for data sharing to healthcare providers or researchers or trusted authorities. Patients share permissions to the healthcare providers in accessing their health records for personal cause. Blockchain systems, especially public and permissionless ones, can face limitations in terms of storage capacity and performance.

Cloud servers provide a scalable solution, allowing blockchain networks to store a large volume of data efficiently. Cloud servers offer robust data backup and redundancy mechanisms, ensuring that data stored on the blockchain system remains highly available even in the event of a failure in the blockchain network.

I. Data Sharing Mechanism

The approach of decentralization in transforming the healthcare will lead to mitigating fragmentation among healthcare providers. However, through this blockchain-driven standardization framework (BDSF) act as a common platform where multiple nodes(users) can interact and share data securely without needing to rely on a central intermediary. The consensus mechanism, such as Proof of Work or Proof of Stake, guarantees the validation of transactions by the network, thereby enhancing trust and security [9]. Furthermore, the process of sharing data among stakeholders is sensitive in the healthcare system, but the inclusion of security measures in the system ensures the integrity of the data and builds trust, enhancing the credibility of medical record sharing among users of the platform.

IV. CONCLUSION

The healthcare in local community hospitals is in traditional way of managing the patients' health record, the inefficiency and the keeping and retrieving of records is a repeated burden among the healthcare providers. Data sharing is one of the issues where processes are not feasible in the system but based on the assessment that sharing of data should be considered to be innovated. Meanwhile, digitalization of healthcare revealed that data sharing among healthcare providers, doctors and patients are quite challenging as well as the authentication of the stakeholders. However, the planned framework with the integration of multiple security measures are significant which allows the local community increase their trust in the public community hospital services. The IS4H tool is also helpful in gathering the data from the respondents. The implication of these solutions based on the findings, are unlocking digitalization for a robust data sharing in healthcare by utilizing the DPID and access control for the security and privacy which will be a great opportunity to have a quality of healthcare services in local community hospitals.

REFERENCES

[1] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," Sustain Cities Soc, vol. 39, pp. 283–297, May 2018, doi: 10.1016/J.SCS.2018.02.014.

[2] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, "Blockchain Application in Healthcare Systems: A Review," Systems, vol. 11, no. 1. MDPI, Jan. 01, 2023. doi: 10.3390/systems11010038.

[3] V. Gilbert, T. Ulep, J. Uy, L. Daryll, D. Casas, and C. E. L. Nuevo, "Assessment of the Service Capability and Readiness of Philippine Hospitals to Provide High-Quality Health Care." [Online]. Available: https://www.pids.gov.ph

[4] Department of Health, "Philippine Health Facility Development Plan 2020-2040 - Annex A," Health Facility Development Bureau, pp. 1–117, 2020.

[5] N. Enterprise Agency, "Health Care in The Philippines Commissioned by the Netherlands Enterprise Agency."

[6] F. K. Nishi et al., "Electronic Healthcare Data Record Security Using Blockchain and Smart Contract," J Sens, vol. 2022, 2022, doi: 10.1155/2022/7299185.

[7] A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," IEEE Access, vol. 7, pp. 147782–147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[8] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives," Cryptography 2019, Vol. 3, Page 3, vol. 3, no. 1, p. 3, Jan. 2019, doi: 10.3390/CRYPTOGRAPHY3010003.

[9] Y. Chen, L. Meng, H. Zhou, and G. Xue, "A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection," Wirel Commun Mob Comput, vol. 2021, 2021, doi: 10.1155/2021/6685762.

[10] M. Tahir, M. Sardaraz, S. Muhammad, and M. S. Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics," Sustainability (Switzerland), vol. 12, no. 17, Sep. 2020, doi: 10.3390/SU12176960.

[11] A. G. Alzahrani, A. Alhomoud, and G. Wills, "A Framework of the Critical Factors for Healthcare Providers to Share Data Securely Using Blockchain," IEEE Access, vol. 10, pp. 41064–41077, 2022, doi: 10.1109/ACCESS.2022.3162218.

[12] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," Health Informatics J, vol. 25, no. 4, pp. 1398–1411, Dec. 2019, doi: 10.1177/1460458218769699.

[13] X. Wang, "Design and Implementation of a Data Sharing Model for Improving Blockchain Technology," Advances in Multimedia, vol. 2022, 2022, doi: 10.1155/2022/4578525.

[14] S. T. Jagtap, C. M. Thakar, O. El Imrani, K. Phasinam, S. Garg, and R. J. M. Ventayen, "A Framework for Secure Healthcare System Using Blockchain and Smart Contracts," in Proceedings of the 2nd International Conference on Electronics and Sustainable Communication Systems, ICESC 2021, Institute of Electrical and Electronics Engineers Inc., Aug. 2021, pp. 922–926. doi: 10.1109/ICESC51422.2021.9532644.

[15] A. R. Lee, M. G. Kim, and I. K. Kim, "SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR," in 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), IEEE, Nov. 2019, pp. 1087–1090. doi: 10.1109/BIBM47256.2019.8983415.

[16] M. Shah, C. Li, M. Sheng, Y. Zhang, and C. Xing, "CrowdMed: A Blockchain-Based Approach to Consent Management for Health Data Sharing," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019. doi: 10.1007/978-3-030-34482-5_31.

[17] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," Comput Struct Biotechnol J, vol. 16, pp. 267–278, Jan. 2018, doi: 10.1016/J.CSBJ.2018.07.004.

[18] "Information Systems for Health (IS4H) TOOLKIT IS4H Maturity Assessment tool Maturity Assessment tool-Version 2.0 IS4H Maturity Assessment tool IS4H-MM 2.0." [Online]. Available: http://www.paho.org/ish