A Decentralized Health Data Repository for Remote Patient Monitoring Using Blockchain and FHIR

Marcos Alves Vieira[1,2], **Gislainy Crisostomo Velasco**[2], **Sergio T. Carvalho**[2]

[1]Instituto Federal de Educação, Ciência e Tecnologia Goiano (IF Goiano)
Iporá – GO – Brasil

[2]Instituto de Informática – Universidade Federal de Goiás (UFG)
Goiânia – GO – Brasil

marcos.vieira@ifgoiano.edu.br, gislainycrisostomo@discente.ufg.br

sergiocarvalho@ufg.br

Abstract. *The world's aging population increasingly faces challenges in accessing healthcare due to a shortage of healthcare professionals. Telemedicine and remote patient monitoring solutions offer a promising avenue for improving access to care, allowing for the monitoring of physiological data, activities performed, and the conditions of the patient's environment. However, such systems must address numerous challenges, such as interoperability, security, integrity, and confidentiality of medical data. In this paper, we propose a repository architecture for medical data obtained through remote patient monitoring. Our solution relies on the Fast Healthcare Interoperability Resources (FHIR) standard to address interoperability issues, while the inherent characteristics of blockchain technology provide security, integrity, and confidentiality of stored data. In addition to remote patient monitoring, the proposed repository has the potential to be used for scientific research, data mining and analysis applications among other health applications. Ongoing implementation and testing of the repository in a real-world setting will demonstrate its performance and scalability. Meanwhile, we present the architecture and constituent elements, including data flow and smart contracts, with their responsibilities described. Overall, our proposed solution offers a promising approach to addressing the challenges of remote patient monitoring and storing medical data securely and efficiently.*

1. Introduction

The growth of the elderly population is a global phenomenon, not limited to developed countries. Projections by the World Health Organization (WHO) suggest that by 2050, the proportion of elderly people will exceed one-fifth of the world population [WHO 2017]. To address this growth, WHO recommends measures such as the prevention and treatment of chronic diseases associated with aging and the development of services that make the elderly's daily lives easier. However, according to WHO projections [WHO 2016], by 2030 there will be a deficit of 14.5 million health professionals. This implies that the population will continue to grow, along with an increase in the number of elderly people, while there will be a simultaneous increase in the shortage of health professionals.

One possible solution to address this problem is Home Care (HC), which reduces treatment costs and is a less intrusive approach [Chelongar and Ajami 2021]. Additionally, HC increases patient engagement by allowing them to continue treatment at home, where they can also carry out other daily activities in parallel [Lundereng et al. 2021].

Telemedicine is another strategy to provide healthcare to people who are bedridden, have mobility difficulties, live in remote areas, or have insufficient access to health professionals [Portnoy et al. 2020]. Telemedicine enables healthcare professionals to remotely monitor, diagnose, and treat patients, offering low-cost services, reducing the need for in-person visits, and minimizing the workforce shortage of healthcare professionals [Rimsza et al. 2015]. By adopting telemedicine, the risk of exposing physicians, other professionals, or patients to contagious diseases, such as the COVID-19 virus, can be reduced [Portnoy et al. 2020, Ahmad et al. 2021].

Recent technological advances make it possible to remotely monitor patients' physiological data (blood pressure, body temperature, heart rate, glycemic index, blood oxygen saturation, etc.), activities (walking, sleeping, eating, etc.), and environmental conditions such as temperature and humidity [Malasinghe et al. 2019, de Farias et al. 2020]. Such measurements are usually performed using medical devices, called Personal Health Devices (PHDs), which may be wearable or not and communicate via wireless data transmission technologies with a device called Personal Health Gateway (PHG), located in the patient's home.

However, a remote patient monitoring environment may be composed of diverse and heterogeneous devices, each using its own data format, making it difficult to integrate them with the Health Information Systems (HIS) of hospitals or clinics where patients' Electronic Health Records (EHR) are stored. Moreover, ensuring the security, integrity, and confidentiality of stored data is crucial, as they are vulnerable to internal and external access breaches that compromise their reliability and availability.

This paper proposes a repository architecture for health data obtained through remote patient monitoring. To mitigate the aforementioned problems, we propose to store the collected data in a blockchain using the Fast Healthcare Interoperability Resources (FHIR)[1] format, with support for cloud integration. The adoption of the FHIR standard ensures interoperability of health data, while blockchain technology has inherent characteristics such as immutability, auditability, security, identity assurance, fault tolerance, and the absence of central authority [Shetty et al. 2017, Hu et al. 2020, Margheri et al. 2020], that can help to address the other aforementioned challenges.

In addition to supporting medical decision-making through remote patient monitoring, the repository can be used for other purposes, such as scientific research or data mining and analysis applications. It is worth noting that any access to health data stored in the repository must be previously authorized by the patient, which, according to the laws of several countries, including the Brazilian General Law of Personal Data Protection (*Lei Geral de Proteção de Dados Pessoais* - LGPD) [Brasil 2018], is the owner of their health information and, therefore, it is their responsibility to consent to its access by third parties.

The remainder of this paper is organized as follows: Section 2 presents the theoretical and technological bases that this work relies on; In Section 3 there is an analysis of the related works and a brief discussion relating them to our proposal; Section 4 provides

[1]https://www.hl7.org/fhir/

a breakdown of the health data repository, as well as examples of its application; Section 5 explores the potential benefits of using smart contracts and blockchain technology in the proposed scenarios, as well as new use cases that could be enabled by our approach. Additionally, we highlight the strengths of our proposal compared to other available alternatives. Finally, in Section 6 the final considerations are outlined, including possibilities for future work.

2. Theoretical Background

Electronic Health Records (EHRs) are an information standardization model that enables integration between different health service providers, making them an essential part of modern healthcare systems [Heart et al. 2017]. One of the primary advantages of using EHRs is their ability to support prescription drug management [Chen 2016], which can help improve patient safety and reduce medication errors [Han et al. 2016]. EHRs also facilitate better disease management by enabling healthcare professionals to access a patient's medical history more easily [Roumia and Steinhubl 2014].

In contrast to EHRs, Personal Health Records (PHRs) are designed to be managed and maintained by patients themselves [Roehrs et al. 2017]. This means that patients can enter their own health data, such as weight or blood pressure measurements, into the record [George and Hopla 2015]. As a result, PHRs can provide valuable health monitoring and epidemiological surveillance capabilities, as well as enabling patients to take a more active role in their own healthcare.

Fast Healthcare Interoperability Resources (FHIR) is a standard created by Health Level Seven International (HL7) to describe data and elements for health data exchange. The FHIR standard is an evolution of HL7 v2, HL7 v3, and HL7 CDA, aiming to facilitate the implementation of a standard for health data interoperability. FHIR solutions are built from a set of modular components called *Resources*, which are a collection of information models that define the data elements, constraints, and relationships for the most relevant healthcare *business objects*. FHIR is currently a widely adopted health information standard and should not be seen as a type of EHR or PHR, as its purpose is only to describe the format of the data and data elements that constitute EHRs or PHRs [Lee et al. 2021].

The concept of blockchain was first introduced by Satoshi Nakamoto [Nakamoto 2008], which is a structure of blocks that store data. Each block, except the first one called the genesis block, contains a hash value of the previous block, forming an unbreakable chain that guarantees the integrity of the entire blockchain. The immutability property of the blockchain comes from the fact that any modification in a block would alter its hash value, breaking the chain structure and invalidating the subsequent blocks. The blockchain is designed to be distributed, where every network node maintains a copy of the entire blockchain, ensuring the system's reliability and fault-tolerance. Consensus among network nodes is necessary to add a new block to the blockchain, enabling a decentralized approach with no central authority. This feature enhances trust among network participants since they can rely on the blockchain's consensus mechanism rather than trusting individual nodes.

Szabo [Szabo 1997] introduced the concept of smart contracts, which are self-executing contracts with terms directly written into code, allowing for the automation of business processes and establishing trust between parties. Smart contracts are similar to physical contracts, where clauses describe actions that must be performed upon certain events. The Ethereum network is an example of a blockchain that treats smart contracts as first-class entities [Nofer et al. 2017, Buterin 2014]. Smart contracts can be used to automate tasks such as verifying insurance claims and facilitating payments, reducing the need for intermediaries and increasing transparency [Swan 2015]. In healthcare, smart contracts could be used to automate the process of granting access to patient data or to manage the delivery of healthcare services, improving efficiency and reducing costs [Zhang et al. 2018a]. Through smart contracts, trust can be established between parties without the need for a third party (*e.g.*, a notary), since the blockchain itself provides the guarantee that the smart contract will be executed as soon as its prerequisites are met.

Combining blockchain and healthcare can result in numerous benefits, including but not limited to improved security and privacy, enhanced data sharing, more efficient data management, and trustless automation of contractual clauses. However, there are also challenges to be addressed, such as regulatory compliance, interoperability with existing systems, and patient consent. The next sections will detail the proposed solution, which aims to address some of these challenges.

3. Related Work

One of the most well-known health data sharing systems is MedRec [Azaria et al. 2016], developed by researchers from Harvard University and the Massachusetts Institute of Technology (MIT). MedRec utilizes the Ethereum blockchain to connect global patients to their health records, which are held by multiple providers. Patients interact with providers through smart contracts on MedRec to view their data. Additionally, patients themselves can control access to their health data via smart contracts.

FHIRChain [Zhang et al. 2018b] is a blockchain and Fast Healthcare Interoperability Resources (FHIR)-based architecture that complies with the scalable sharing and security requirements[2] defined by the United States' Office of the National Coordinator for Health Information Technology (ONC), which is similar to Brazil's Informatics Department of the Unified Health System (DATASUS)[3].

OmniPHR [Roehrs et al. 2017] proposes a patient-centered blockchain that emphasizes the benefits of Personal Health Records (PHR) – more details on PHR and Electronic Health Records (EHR) can be found in Section 2. Patient data is recorded in encrypted hierarchical blocks, signed by the entity responsible for its insertion (*e.g.*, provider, patient, or medical device). The data can be stored either on-chain within the blockchain or off-chain externally. In the latter case, OmniPHR maintains pointers to the location of the data rather than the data itself.

Other works, such as Celestrini *et al.* [Celestrini et al. 2019] and Barbosa *et al.* [Barbosa et al. 2020], utilize Personal Health Devices (PHDs) to monitor patient health, with or without the use of cloud computing. Barbosa *et al.*'s work is focused on the Brazilian data model for representing EHRs and describes an application scenario for its proposal to detect possible cases of COVID-19.

Our proposal for remote patient monitoring includes a health data repository that

[2] https://www.healthit.gov/topic/interoperability/interoperability-roadmap
[3] https://datasus.saude.gov.br/

shares similarities with the works mentioned in this section. The patient's PHDs send data to a device called a Personal Health Gateway (PHG) located in their home. The PHG then converts each patient's raw device data to the FHIR standard and uses a specific smart contract to record this FHIR file on the blockchain. To enhance scalability, we can store only a pointer to the actual data in the repository and keep it off-chain in a cloud storage service. Third parties such as healthcare professionals can consult the patient's data stored in the repository by executing the smart contract developed exclusively for this purpose, once the patient grants access. In the following section we provide more details about how the repository works.

4. Proposal

In this section we outline the proposed health data repository, along with some examples of how its stored data can be used in practical applications.

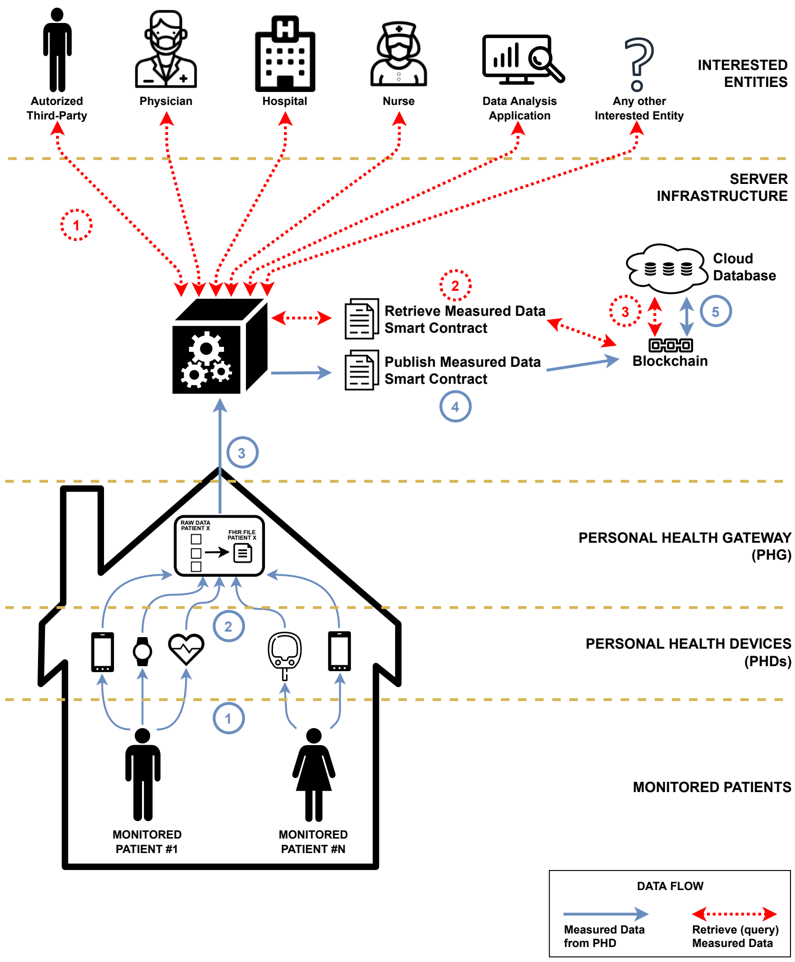

Figure 1. Health data repository architecture.

4.1. Health Data Repository for Remote Patient Monitoring

The components of the health data repository for remote patient monitoring are depicted in Figure 1. The flow of publishing data measured by the medical devices is represented by continuous blue arrows, while the flow of querying the repository is represented by red dashed arrows. The numbers indicate the sequence of publishing and querying operations.

To refer to the medical devices for monitoring vital signs and the device to which the PHDs are connected and where their measurements are sent, we adopt the terminology established in the Personal Connected Health Alliance (PCHAlliance) guidelines[4]. These devices are denoted as Personal Health Devices (PHDs) and Personal Health Gateway (PHG), respectively. However, the operation of the repository is not restricted to working only with devices certified by PCHAlliance. Therefore, a remote patient monitoring environment is composed of the patients, their PHDs, and at least one PHG. The components of the repository and their details are presented in the following sections.

4.1.1. Monitored Patients

Individuals whose vital signs and physical activities are being monitored by medical devices, whether they are wearable or not, are referred to as "monitored patients."These devices are known as Personal Health Devices (PHDs). To ensure that the collected data can be unambiguously associated with a single patient throughout the repository, patients must have a universally unique identifier (UUID) [ISO/IEC 9834-8 2014], which is used to identify the measurements made by their PHDs.

4.1.2. Personal Health Devices (PHDs)

Personal Health Devices (PHDs) are devices that can be wearable or non-wearable and are used to measure physiological data or physical activities. These measurements are then transmitted wirelessly to the Personal Health Gateway (PHG) using technologies such as WiFi or Bluetooth. Examples of PHDs include glucose meters, blood pressure or heart rate monitors, scales, and even motion or fall sensors. PHCAlliance provides a list of certified PHDs on their website[5].

4.1.3. Personal Health Gateway (PHG)

The Personal Health Gateway (PHG) is responsible for collecting data sent by PHDs in a remote patient monitoring environment. It can take the form of an exclusive device designed solely for this purpose, or it can be an application for mobile devices or computer software installed on the patient's cell phone, tablet, or computer.

Its purpose in the repository is to receive the raw data forwarded by the PHDs in the environment and package them into a single FHIR file, representing a Personal Health Record (PHR). The PHR may contain one or several measurements from one or more devices. After the PHR is built under FHIR format, it is forwarded to the blockchain, triggering the smart contract for data publication.

The frequency at which data is forwarded to the blockchain and other settings are configurable in the PHG, such as whether the data from each device should be stored in a separate PHR, or if it should be stored *off-chain* (*e.g.*, in the cloud) and only its pointer

[4]https://www.pchalliance.org/continua-design-guidelines
[5]https://www.pchalliance.org/product-showcase

should be stored in the blockchain. In the latter case, the files' hashes stored in an *off-chain* method compose the PHR, as a way to ensure data integrity, that is, the possibility of checking whether these files have been tampered with or not.

The PHR data model is illustrated in Figure 2. Its components are the FHIR resources: `Composition`, occurring only once and comprising one or several `Observation` elements. Each Observation element refers to a single `Patient` and `Device` and can refer to one or more `Media` elements. All of these, are, in turn, packaged into a `Bundle` resource.

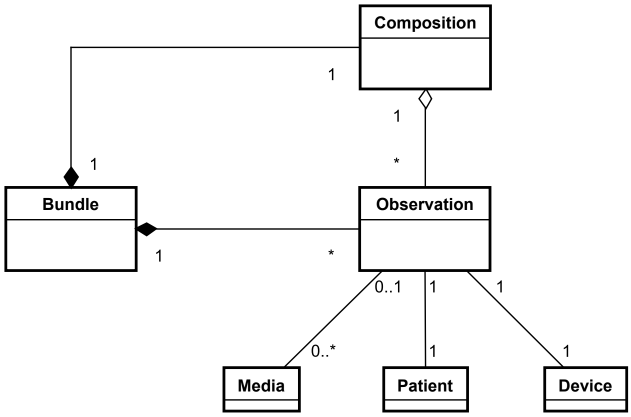

Figure 2. FHIR resources that constitute the Personal Health Record (PHR) data model.

4.1.4. Server Infrastructure

The server infrastructure of the repository is a key component of the proposed solution, providing the necessary capabilities for secure and efficient storage and access of medical data obtained through remote patient monitoring. The infrastructure is built using the Hyperledger Fabric blockchain[6], a distributed ledger technology that offers a high level of security and transparency. The infrastructure consists of three smart contracts and their access API, represented by the cube with gears in the center of Figure 1. This is an adapted version of the blockchain architecture introduced by [Vieira and Carvalho 2021].

The first two smart contracts are responsible for publishing and querying data in the repository. When a new FHIR file is received for publishing, the repository performs a validation process to ensure the file's integrity and adherence to the FHIR standard before triggering the publishing smart contract. The query smart contract, on the other hand, only performs searches on the repository data if the requesting entity owns a valid access grant. This ensures that patient privacy is maintained, and the data can only be accessed by authorized entities.

Furthermore, patients have the ability to grant or revoke access to their data through a third smart contract. This allows patients to control who has access to their medical information and ensures that the data is only used for authorized purposes. The

[6]https://www.hyperledger.org/use/fabric

process of granting access to third parties is described in more detail in the following section. Overall, the infrastructure provides a robust and secure platform for the storage and management of medical data, ensuring patient privacy and data integrity.

4.1.5. Interested Entities

Access to patient data stored in the repository is strictly regulated to ensure patient privacy and data confidentiality. As such, entities interested in accessing patient data must follow a strict authorization process. This involves triggering the repository's third smart contract designed for granting and revoking access to data through UUIDs. The smart contract verifies the requesting entity's access authorization before allowing access to a patient's data. This access authorization is verified using public-key cryptography, where the patient's private key is used to grant access to authorized entities. Thus, when an entity requests access to a patient's data, the repository verifies the entity's access authorization by checking its digital signature against the patient's public key. If the signature is valid, the repository performs the query and sends the data to the entity using the FHIR standard. Once verified, the entity can query the repository using the FHIR standard to retrieve patient data.

Entities that may be interested in accessing patient data include healthcare professionals and data analysis applications. Healthcare professionals can use the patient data to monitor their patients' conditions remotely, analyze trends in patient health, and make informed treatment decisions. Data analysis applications can use the repository's data to train machine learning models for predicting patient outcomes or identifying patterns in patient health that can inform disease prevention and management strategies.

The access authorization process is a crucial aspect of the repository's architecture, and it is designed to prevent unauthorized access to patient data. This process is based on the blockchain architecture introduced by [Vieira and Carvalho 2021], which provides a secure and transparent method for managing access to patient data. By using a blockchain-based approach, the repository ensures that patient data is accessed only by authorized entities, and access events are recorded on the blockchain for audit and traceability purposes.

4.2. Examples of Applications

In this section, we provide examples of applications that can benefit from the data stored in the health data repository.

4.2.1. Remote Patient Monitoring at Home

In [Vieira and Carvalho 2016a, Vieira and Carvalho 2016b], we present a scenario in which an elderly couple lives in a smart home equipped with wearable medical devices that monitor their vital signs. Other PHDs, such as a digital scale, motion sensors, and smart locks, are also deployed throughout the house, as shown in Figure 3. These PHDs are connected to a personal health application that aims to monitor the couple's vital signs and send them reminders to take their medications on time, perform regular physical activity, or check their weight on the digital scale.

In this scenario, the personal health application acts as a Personal Health Gateway (PHG), collecting the data from the distributed PHDs in the house. This application can easily be adapted to convert the data measured by the PHDs into the FHIR format and submit it to the repository. Once in the repository, physicians or even family members can monitor the couple's vital sign measurements, physical activity, and adherence to their medication prescriptions, subject to prior authorization by the patients.

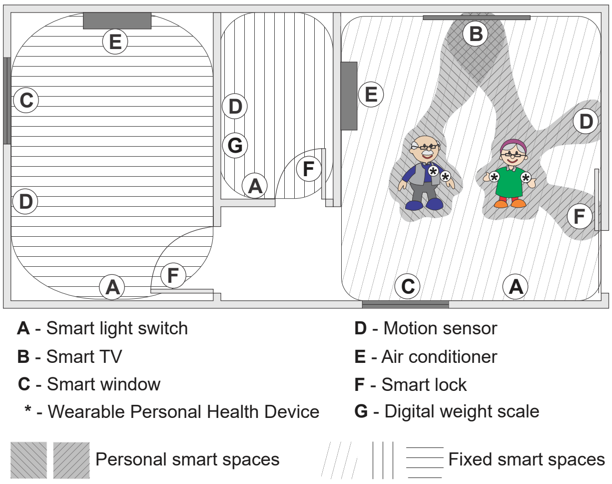

Figure 3. Smart home with elderly couple using wearable and non-wearable PHDs. Adapted from [Vieira and Carvalho 2016a, Vieira and Carvalho 2016b].

A possible application of the health data repository is an emergency detection system that continuously monitors specific PHDs of a patient, such as a blood pressure monitor or fall sensor, and alerts nearby emergency services or designated relatives in case of an emergency.

4.2.2. Telemedicine

The provision of services through telemedicine has been defined by the Brazilian Federal Council of Medicine (*Conselho Federal de Medicina* - CFM) since 2002, through CFM Resolution 1.643/2002 [CFM 2002]. However, the COVID-19 pandemic has led to an increased adoption of telehealth and telemedicine technologies, which provide secure communication channels for physicians and healthcare specialists, minimizing the spread of infection [Ahmad et al. 2021] and allowing moderately ill patients to receive the necessary healthcare while minimizing exposure to severely ill patients [Portnoy et al. 2020]. Therefore, the Brazilian Federal Government has regulated the use of telemedicine during the COVID-19 pandemic through Law 13.989/2020 [Brasil 2020].

The proposed health data repository can assist in medical decision-making during teleconsultations, especially in the triage of patients suspected of having COVID-19 or those recovering from it, by providing current and historical data from PHDs that monitor temperature, heart rate, or blood oxygen saturation. This information is crucial for determining the severity of the patient's condition and guiding the medical team in deciding the best course of action. Additionally, the repository can store medical exam images and videos, such as X-rays and ultrasounds, which can be accessed remotely by specialists during teleconsultations.

4.2.3. Health Data Mining

Data mining technology enables the search for potentially valuable knowledge in a large volume of data. Health data mining can facilitate the acquisition of effective knowledge of patient diagnosis and treatment, increase the accuracy of disease prediction, detect diseases at an early stage, and improve the cure rate [Yang et al. 2020].

Upon the adoption of the health data repository proposed in this work, it is anticipated that it will be fueled by data from numerous patients. Such data can be examined by government agencies in an anonymized manner, without identifying the patient[7] to assess the adoption of health or epidemiological surveillance measures. Research institutions can utilize the data in the repository (anonymized or subject to patients' consent) to conduct research, for example, on the effectiveness of new drugs or vaccines.

5. Discussion

The proposed blockchain-based repository's goal is to offer a secure, decentralized, and interoperable solution for health data management with potential applications in various health contexts, *e.g.* [Swan 2015, Azaria et al. 2016, Dagher et al. 2018]. The blockchain technology provides security and immutability of data, making it practically impossible to modify the data stored in the repository without detection. Moreover, the decentralized nature of blockchain technology enables data sharing and access control without relying on a central authority or intermediary, reducing the risk of data breaches and unauthorized access. The use of smart contracts in the proposed repository allows for the implementation of automated and transparent data access and consent management. The adoption of the FHIR standard enables interoperability with existing healthcare systems and applications, facilitating data exchange and integration with electronic health records and other health IT solutions.

In comparison to other proposed systems for remote patient monitoring, our proposal has unique strengths. The use of the FHIR standard allows for increased interoperability and compatibility with existing health information systems. The use of blockchain technology provides security, immutability, and decentralization of data, which are essential features for health data management. Additionally, our proposal includes the use of smart contracts to manage access to the data stored in the repository, providing more control and transparency over data sharing and access. Finally, our proposal illustrates the potential of the repository in supporting various health applications, such as telemedicine and health data mining, which can have a significant impact on improving patient care and disease management.

In addition to the scenarios proposed in the previous sections, there are other health applications that can benefit from the proposed blockchain-based repository. One

[7] Article 5 of the Brazilian General Law of Personal Data Protection (*Lei Geral de Proteção de Dados Pessoais* - LGPD) [Brasil 2018] defines "anonymized data" as "data pertaining to a subject who cannot be identified, considering the use of reasonable and available technical means at the time of its treatment".

such application is clinical trials. Clinical trials involve the collection of large amounts of data from patients over extended periods of time. The use of a blockchain-based repository can provide a secure and transparent environment for managing this data, ensuring that the data is not tampered with or lost, and that all parties have access to the same version of the data. Smart contracts can be used to enforce data privacy and access control rules, ensuring that only authorized parties can access the data.

Another potential application is public health surveillance. Public health surveillance involves monitoring the incidence and prevalence of diseases in a population. The use of a blockchain-based repository can provide a centralized and secure platform for storing and analyzing public health data. Smart contracts can be used to ensure that data privacy is maintained, and that only authorized parties have access to the data.

Finally, the proposed repository can also be used for medical research. Medical research involves the collection and analysis of large amounts of data from various sources. The use of a blockchain-based repository can provide a secure and transparent environment for managing this data, ensuring that the data is not tampered with or lost, and that all parties have access to the same version of the data. Smart contracts can be used to enforce data privacy and access control rules, ensuring that only authorized parties can access the data.

Our repository can store the patient's vital signs, symptoms, and treatment history in the scenario of home remote patient monitoring. Authorized healthcare providers can access this data securely through the blockchain network, using their private keys to retrieve patient information. Smart contracts can also be used to automate the payment process for these services, ensuring transparency and efficiency. In the case of telemedicine, our repository can provide a secure and reliable platform for exchanging patient data between healthcare providers and patients. Smart contracts can enforce data access permissions, ensuring that only authorized parties can access the data. The blockchain provides a tamper-proof audit trail of all data transactions, useful for regulatory compliance and legal disputes. Finally, our repository can be used to extract valuable knowledge from a large volume of patient data in the scenario of health data mining. Smart contracts can enforce data privacy and anonymization rules, ensuring that patient data is only used for authorized research purposes.

In summary, the proposed blockchain-based repository offers a secure, transparent, and interoperable platform for managing health data in various health contexts. It has the potential to benefit applications such as clinical trials, public health surveillance, medical research, and remote patient monitoring. Our approach offers advantages over traditional approaches, including increased data interoperability, security, integrity, auditability, and automation of data access and publication, potentially improving healthcare delivery and patient outcomes.

6. Concluding Remarks

The use of telemedicine and home care can help maximize access to health care for the population, especially in times of pandemics such as COVID-19. However, such health strategies are highly technology-dependent and their implementation can raise a myriad of challenges. Estimates from the World Health Organization (WHO) indicate that the percentage of elderly people in the world population tends to grow in the next decades and, on the counterpoint, the deficit of health professionals also tends to increase.

In response to these challenges, in this paper, we proposed a repository of health data collected from remote patient monitoring as a way to support medical decision-making regarding the monitored patients. The data is stored in the repository in FHIR format – a widely used health data standard – as a way to ensure increased interoperability. The repository is built on top of a blockchain architecture, taking advantage of its inherent characteristics, such as security, integrity, auditability, and decentralization.

The proposed repository can support a variety of applications in the field of health care. For instance, in the scenario of home remote patient monitoring, the repository can assist medical decision-making by providing current and historical health data such as temperature, heart rate, or blood oxygen saturation. In the context of telemedicine, the repository can store images and videos from medical exams, such as X-rays and ultrasounds, which can be accessed remotely by specialists during teleconsultations. Additionally, the repository can assist in health data mining by providing effective knowledge of patient diagnosis and treatment, increasing the accuracy of disease prediction, detecting diseases at an early stage, and increasing the cure rate.

While this study presents a comprehensive overview of the proposed solution and its potential applications, the implementation and testing of the repository are currently underway. The next step is to conduct further research and development to test the performance and scalability of the proposed solution in a real-world setting. The results of the implementation and tests will be published in a future work. Furthermore, we plan to implement data provenance functionalities, similar to those proposed in [Vieira and Carvalho 2021], to monitor access to the repository data by authorized entities, providing auditing capabilities of the use of the data stored in the repository.

In conclusion, the proposed health data repository can provide significant benefits in various health scenarios, including remote patient monitoring, telemedicine, and health data mining. By leveraging the advantages of blockchain technology, such as security, integrity, auditability, and decentralization, the repository can enhance medical decision-making and contribute to the development of health policies and research initiatives. Ultimately, this repository can positively impact the population by fostering progress in the field of healthcare.

References

[Ahmad et al. 2021] Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., and Omar, M. (2021). The role of blockchain technology in telehealth and telemedicine. *International Journal of Medical Informatics*, 148:104399.

[Azaria et al. 2016] Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30.

[Barbosa et al. 2020] Barbosa, V., Ferreira, H., Gomes, L., Gomes, F., Barreto, I., Monteiro, O., and Oliveira, M. (2020). SmartRES - Uma plataforma IoT para Monitoramento Inteligente em Saúde e sua Aplicação no Contexto da COVID-19. In *Anais do XX Simpósio Brasileiro de Computação Aplicada à Saúde*, pages 297–307, Porto Alegre, RS, Brasil. SBC.

[Brasil 2018] Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. *Diário Oficial [da] República Federativa do Brasil*.

[Brasil 2020] Brasil (2020). Lei nº 13.989, de 15 de abril de 2012. *Diário Oficial [da] República Federativa do Brasil*.

[Buterin 2014] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. White Paper. Available online: `https://ethereum.org/en/whitepaper/`.

[Celestrini et al. 2019] Celestrini, J., Rocha, R., Santos, C., Mota, V., Filho, J., and Andreão, R. (2019). HealthDash: Monitoramento remoto de pacientes utilizando programação baseada em fluxo de dados. In *Anais do XIX Simpósio Brasileiro de Computação Aplicada à Saúde*, pages 222–233, Porto Alegre, RS, Brasil. SBC.

[CFM 2002] CFM, Conselho Federal de Medicina. (2002). Resolução CFM nº 1.643, de 26 de agosto de 2002. *Diário Oficial [da] República Federativa do Brasil*.

[Chelongar and Ajami 2021] Chelongar, K. and Ajami, S. (2021). Using active information and communication technology for elderly homecare services: A scoping review. *Home Health Care Services Quarterly*, 40(1):93–104. PMID: 32990180.

[Chen 2016] Chen, R. (2016). Current challenges of ehrs for oncologists. *Oncology Times*, 38(16).

[Dagher et al. 2018] Dagher, G. G., Mohler, J., Milojkovic, M., and Marella, P. B. (2018). Blockchain: The evolution of decentralized system architectures. *IEEE Access*, 6:5306–5320.

[de Farias et al. 2020] de Farias, F. A. C., Dagostini, C. M., de Assunção Bicca, Y., Falavigna, V. F., and Falavigna, A. (2020). Remote Patient Monitoring: A Systematic Review. *Telemedicine and e-Health*, 26(5):576–583.

[George and Hopla 2015] George, T. P. and Hopla, D. L. (2015). Advantages of personal health records. *Nursing2020 Critical Care*, 10(6).

[Han et al. 2016] Han, J. E., Rabinovich, M., Abraham, P., Satyanarayana, P., Liao, T. V., Udoji, T. N., Cotsonis, G. A., Honig, E. G., and Martin, G. S. (2016). Effect of Electronic Health Record Implementation in Critical Care on Survival and Medication Errors. *The American Journal of the Medical Sciences*, 351(6):576–581.

[Heart et al. 2017] Heart, T., Ben-Assuli, O., and Shabtai, I. (2017). A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy. *Health Policy and Technology*, 6(1):20–25.

[Hu et al. 2020] Hu, R., Yan, Z., Ding, W., and Yang, L. T. (2020). A survey on data provenance in IoT. *World Wide Web*, 23(2):1441–1463.

[ISO/IEC 9834-8 2014] ISO/IEC 9834-8 (2014). Information technology – Procedures for the operation of object identifier registration authorities – Part 8: Generation of universally unique identifiers (UUIDs) and their use in object identifiers. Standard, International Organization for Standardization, Geneva, CH.

[Lee et al. 2021] Lee, Y.-L., Lee, H.-A., Hsu, C.-Y., Kung, H.-H., and Chiu, H.-W. (2021). Implement an International Interoperable PHR by FHIR—A Taiwan Innovative Application. *Sustainability*, 13(1).

[Lundereng et al. 2021] Lundereng, E. D., Nes, A. A. G., Holmen, H., Winger, A., Thygesen, H., Jøranson, N., Borge, C. R., Chen, W., Dajani, O., Mariussen, K. L., and Steindal, S. A. (2021). Health care professionals' experiences and perspectives on using telehealth for home-based palliative care: Protocol for a scoping review. *JMIR Res. Protoc.*, 10(10):e33305.

[Malasinghe et al. 2019] Malasinghe, L. P., Ramzan, N., and Dahal, K. (2019). Remote patient monitoring: a comprehensive study. *Journal of Ambient Intelligence and Humanized Computing*, 10(1):57–76.

[Margheri et al. 2020] Margheri, A., Masi, M., Miladi, A., Sassone, V., and Rosenzweig, J. (2020). Decentralised provenance for healthcare data. *International Journal of Medical Informatics*, 141(June):104197.

[Nakamoto 2008] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. White Paper. Available online: https://bitcoin.org/bitcoin.pdf.

[Nofer et al. 2017] Nofer, M., Gomber, P., Hinz, O., and Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3):183–187.

[Portnoy et al. 2020] Portnoy, J., Waller, M., and Elliott, T. (2020). Telemedicine in the Era of COVID-19. *The Journal of Allergy and Clinical Immunology: In Practice*, 8(5):1489–1491.

[Rimsza et al. 2015] Rimsza, M. E., Hotaling, A. J., Keown, M. E., Marcin, J. P., Moskowitz, W. B., Sigrest, T. D., and Simon, H. K. (2015). The Use of Telemedicine to Address Access and Physician Workforce Shortages. *Pediatrics*, 136(1):202–209.

[Roehrs et al. 2017] Roehrs, A., da Costa, C. A., and da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, 71:70–81.

[Roumia and Steinhubl 2014] Roumia, M. and Steinhubl, S. (2014). Improving cardiovascular outcomes using electronic health records. *Current Cardiology Reports*, 16(2):451.

[Shetty et al. 2017] Shetty, S., Red, V., Kamhoua, C., Kwiat, K., and Njilla, L. (2017). Data provenance assurance in the cloud using blockchain. In Hall, R. D., Blowers, M., and Williams, J., editors, *Disruptive Technologies in Sensors and Sensor Systems*, volume 10206, page 102060I.

[Swan 2015] Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.

[Szabo 1997] Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, 2(9).

[Vieira and Carvalho 2016a] Vieira, M. A. and Carvalho, S. T. (2016a). Addressing the Concurrent Access to Smart Objects in Ubiquitous Computing Scenarios. In *Proceedings of the 22nd Brazilian Symposium on Multimedia and the Web*, Webmedia '16, page 79–82, New York, NY, USA. Association for Computing Machinery.

[Vieira and Carvalho 2016b] Vieira, M. A. and Carvalho, S. T. (2016b). (Meta)Modelagem de Espaços Inteligentes Pessoais e Espaços Inteligentes Fixos para Aplicações Ubíquas. In *Anais do VIII Simpósio Brasileiro de Computação Ubíqua e Pervasiva (SBCUP)*, pages 1056–1065, Porto Alegre-RS, Brazil. Sociedade Brasileira de Computação - SBC.

[Vieira and Carvalho 2021] Vieira, M. A. and Carvalho, S. T. (2021). Towards a blockchain-based architecture for data provenance management in the internet of things. In *SBRC 2021 - IV WBlockchain 2021 (IV Workshop em Blockchain: Teoria, Tecnologias e Aplicações)*.

[WHO 2016] WHO, World Health Organization. (2016). Global strategy on human resources for health: Workforce 2030. https://www.who.int/hrh/resources/global_strategy_workforce2030_14_print.pdf. [Online; accessed Jan-2022].

[WHO 2017] WHO, World Health Organization. (2017). 10 facts on ageing and health. https://www.who.int/news-room/fact-sheets/detail/10-facts-on-ageing-and-health. [Online; accessed Jan-2022].

[Yang et al. 2020] Yang, J., Li, Y., Liu, Q., Li, L., Feng, A., Wang, T., Zheng, S., Xu, A., and Lyu, J. (2020). Brief introduction of medical database and data mining technology in big data era. *Journal of Evidence-Based Medicine*, 13(1):57–69.

[Zhang et al. 2018a] Zhang, P., White, J., Schmidt, D. C., and Lenz, G. (2018a). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied Sciences*, 8(7):1225.

[Zhang et al. 2018b] Zhang, P., White, J., Schmidt, D. C., Lenz, G., and Rosenbloom, S. T. (2018b). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational and Structural Biotechnology Journal*, 16:267–278.