Blockchain-based Framework for Health Tourism That Follows the GDPR

Frederico de Pessoa Oliveira
Instituto Superior Técnico
Universidade de Lisboa
Lisboa, Portugal
frederico.oliveira@tecnico.ulisboa.pt

ABSTRACT

Health tourism has grown significantly over the past few decades, with an estimated 20 to 24 million patients crossing borders each year to receive medical treatments. This emerging sector plays a key role in meeting the sensitive and vital needs and desires of health tourists by providing access to affordable healthcare services. However, the industry faces significant challenges: privacy and transparency concerns, lack of access to centralized health records, fraudulent practices, opportunistic behavior of intermediaries and contractual/legal issues. While Blockchain technology has great potential to address and solve many of the industry's inherent challenges and inefficiencies, current understanding of its application in health tourism is fragmented. Furthermore, the technology itself has certain limitations and its implementation poses a number of challenges that must be considered when applying it to the health tourism sector, mainly related to regulatory compliance such as the General Data Protection Regulation.

Therefore, the main purpose of this thesis is to develop a GDPR-compliant Blockchain-based framework for healthcare data management, focused on the specific case of health tourism. Our goal is to help researchers and practitioners understand the requirements for developing GDPR-compliant Blockchain solutions for health tourism practice.

This document studies the practical implications of the GDPR on the development of Blockchain solutions for storing and sharing personal health data, clearly identifies the existing challenges and reviews the solutions proposed in the literature to address them.

KEYWORDS

Blockchain; GDPR; Health Tourism; Personal Data; Health Data; PHR

1 Introduction

Over the past few decades, health tourism has witnessed significant growth, with an estimated 20 to 24 million patients crossing borders each year to receive medical treatments [3, 34, 36]. By health tourism we refer to phenomenon of patients travelling abroad in order to seek or avail medical and allied services and facilities [34]. The health tourism value chain is composed of three main phases: pre-procedure, procedure and post-procedure. Pre-procedure is the first phase of health tourism, which involves preparation by a medical tourist to receive medical service [46]. This phase consists of several important stages, including choice of health travel facilitator, medical providers like hospitals or doctors, and the destination country [3, 34, 46]. The procedure phase, which is the second phase, begins once the patient reaches the destination country [34]. In this phase, the patient visits the hospital, undertakes required tests and consultations, and undergoes treatment or procedure [3]. The post-procedure phase is the last and involves post-operative care and follow-up care of the medical tourists [3, 34, 46].

This emerging sector created a new tourist class by combining healthcare services with tourism and hospitality with access to affordable healthcare services [36]. Affordability, accessibility and availability are considered the primary drivers for searching for alternative healthcare and medical intervention options overseas [36]. The scope of health tourism ranges from medical procedures such as minor dental procedures, cosmetic surgery and significant interventions, often referred to as medical tourism, to the organized travel to maintain, enhance or restore the mind and body's wellbeing, which is referred as wellness tourism [34, 36].

Although it plays a key role in meeting the sensitive and critical needs and desires of health tourists, there are still uncertainties at all stages of the health tourism process, including pre-procedure and post-procedure [46]. There are significant challenges facing the health tourism industry: privacy and transparency concerns, lack of access to centralized medical records, fraudulent practices, opportunistic behavior of intermediaries, foreign currency risks, and contractual/legal issues [3].

Blockchain has been receiving increasing interest in recent years and is considered a disruptive technology [37] with the potential to redefine the way information is stored and disseminated, particularly sensitive information, such as personal health data [24]. Blockchain can address and solve many of the challenges and inefficiencies inherent to the health tourism industry [3, 36, 42]. It offers a distributed and immutable leger for collecting, storing, and processing data [1, 4]. Due to its distributed and immutable nature, Blockchains also enable the transparency, verifiability, and traceability of data stored on-chain [18, 47].

However, the same architecture that grants multiple privacy-friendly qualities to Blockchain [47] is also the one that makes it subject to several different issues, mainly compliance with legal regulations [4]. The introduction of the General Data Protection Regulation (GDPR) brought some challenges to the designing and development of Blockchain solutions and changed the way personal data is perceived [5]. This is primarily due to the fact that during its development the GDPR did not consider emerging decentralized technologies, such as Blockchain [1], which resulted in tension between the technology and the regulation [11].

Furthermore, major legal or regulatory changes always had a great impact on social and economic activities, even more today considering the technological advances, rapid innovation and the increase of system's complexity in many fields. Healthcare is no exception, being extremely impacted by such changes. Accordingly, it came as no surprise that the introduction of GDPR caused an immediate impact on businesses and services that involve the processing and storage of personal data, as is the case of healthcare related activities, such as health tourism.

The GDPR appoints obligations and responsibilities on how organizations collect, store and process personal data, and it requires organizations to be completely transparent with how they use, protect and safeguard that same personal data. In the case of healthcare organizations, this is all the more significant since data concerning health is considered "sensitive data" under the GDPR [2, 16, 27, 30, 31, 51], which benefits from additional protection [31] and stricter requirements. According to Article 4, "data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. In addition, some specific derogations are defined for this type of personal data, aiming at protecting the rights of individuals and the confidentiality of their personal health data, whilst preserving the benefits of processing data [9].

1.1 Research Problem

As discussed above, even though Blockchain is viewed as a technology capable of redefining the way information is stored and disseminated, particularly sensitive information [24], its implementation introduces a significant amount of challenges, encompassing compliance with privacy regulations, privacy issues, and scalability limitations. Thus, the Blockchain must be integrated along with other technologies in order to solve several of these challenges. Further, since compliance with the GDPR must be assessed on a case-by-case basis, there is a need to examine the implications of the regulation on the different types and specific domains of Blockchain applications.

In the particular case of the health tourism industry, some of these concerns become even more increasingly alarming since health data is subject to stricter regulatory, security and legal requirements, a key factor limiting Blockchain adoption in the sector [26]. Although Blockchain technology holds the potential to provide serious improvements for healthcare data management compared with current information management systems, there are inherent issues when integrating traditional Blockchain solutions with healthcare data storage and sharing [26]. That being said, there is a need to assess these specific challenges and the implications of the legal regulations on health data in order to better align Blockchain's capabilities with healthcare data management and, consequently, ease the development of compliant healthcare Blockchain solutions.

1.2 Proposed Solution

To address the identified research problems, we intend to develop a GDPR-compliant Blockchain-based framework for healthcare data management, focused on the specific case of health tourism. The framework will be built on the knowledge gathered from the literature reviews and will serve as support for designing GDPR-compliant blockchain architectures for health tourism. Inside the health tourism domain, we will devote our attention to the fields of medical tourism and wellness tourism.

Our aim with this solution is to provide a widely accepted framework to assist researchers and practitioners in understanding the requirements for developing GDPR-compliant healthcare Blockchain solutions, focused on health tourism. This framework is expected to enable users to own their data and easily share their healthcare data while assuring its privacy and protection, and complying with legal regulations. Moreover, it is meant to tackle existing limitations, such as scalability, and the security and privacy of data stored and transferred.

1.3 Objectives

The objectives to be pursued with this dissertation are:

- To assess existing challenges between Blockchain technology and GDPR, and the review of current techniques and solutions to deal with those same challenges. Thus, we conduct a Systematic Literature Review (SLR) to identify the benefits and challenges of using Blockchain technology to store personal data, and review the current state-of-the-art for implementing GDPR-compliant Blockchain solutions;
  The following three research questions were formulated to guide the review:
  RQ1. What are the main benefits and challenges of using Blockchain technology for storing personal data?
  RQ2. What are the main challenges when implementing GDPR-compliant Blockchain technology?
  RQ3. What is the current state-of-the-art for implementing GDPR-compliant Blockchain solutions?

- To assess the impact and existing implications of the GDPR on healthcare practice and research in order to clarify researchers, healthcare organisations and other institutions that process or intend to process health data of individuals about their obligations under the regulation and the measures that they need to take to fulfil them. Another SLR is performed with the goal of identifying the main benefits and challenges of compliance with the GDPR in the healthcare sector, as well as existing derogations from the regulation;
  The following three research questions were formulated to guide the review:

RQ1. What are the benefits of compliance with the GDPR in the healthcare sector?
RQ2. What are the challenges of compliance with the GDPR in healthcare?
RQ3. What exemptions from the GDPR exist in the healthcare sector?

- To assess current developments on the use of Blockchain for the practice of health tourism. This would support researchers and practitioners in better understanding the full potential of blockchain use in health tourism, increase its acceptability and assist in the implementation of solutions. A Multivocal Literature Review (MLR) is carried out to summarize the existing evidence on both the state-of-the-art and practice on the use of blockchain solutions for health tourism;
  The following research question was formulated to guide the review:
  RQ. What is the current state-of-the-art in the use of Blockchain for health tourism?

1.4 Document Structure

The remainder of this document is organized as follows. Chapter 2 describes the applied research methodologies, detailing the distinct phases that comprise each of the research processes. An overview of the main concepts discussed throughout this investigation is provided in Chapter 3. The literature reviews are conducted in Chapters 4, 5 and 6. Chapter 7 explains how the findings of this investigation were communicated to researchers and other relevant audiences. Finally, the last chapter concludes our work and outlines future research directions.

2 Research Methodology

In this chapter, the research methodologies used to guide the research are described.

2.1 Systematic Literature Review

In this dissertation, two Systematic Literature Reviews (SLR) are conducted following the guidelines and recommendations by [21, 22, 50] A systematic literature review is a means of identifying, evaluating and interpreting all available research relevant to a topic area, or phenomenon of interest. Individual studies contributing to a systematic review are called primary studies while a systematic review is a form a secondary study [21, 22]. This research methodology was selected due to its structured search approach, which provides fairness to the work and seeks to eliminate any research bias [21, 22]. Moreover, since it is a systematic approach and follows a predefined search strategy, it can be easily replicated.
The research process comprises the planning, conducting, and reporting phases as proposed by [21, 22].

2.2 Multivocal Literature Review

A Multivocal Literature Review (MLR) is conducted following the guidelines and recommendations by [12]. A MLR is a form of Systematic Literature Review (SLR) that includes grey literature like blogs, videos, web-pages and white papers, which are constantly produced by SE practitioners outside academic forums, in addition to the published formal literature such as journal articles and conference papers [12]. Therefore, MLRs are important to the expansion of the research by including literature that normally would not be included due to its "grey" nature.
When considering conducting a literature review from formal literature in the specific topic of blockchain in health tourism, the author realized that broadening the scope and including grey literature (GL) would add value and benefits to the study as well as close the gap between academic research and professional practice. It is expected that the GL will provide essential knowledge regarding the use of blockchain for professional practice, but the evidence provided is often based on experience and opinion, so it is understandable that including such relevant literature presents particular challenges.
There are several guidelines in the literature for conducting SLR studies in SE, e.g., [21, 22]. However, several phases of MLRs differ from those of traditional SLRs. In particular, the process of researching and assessing the quality of sources. Therefore, the SLR guidelines are only partially helpful in conducting MLR studies. The research process comprises the planning, conducting, and reporting phases as proposed by [12]

3 Background

In this chapter, relevant background knowledge on Blockchain, GDPR, Electronic Health Records and Personal Health Records is presented.

3.1 Blockchain Technology

The concept of Blockchain was first introduced in [33] as the underlying technology behind Bitcoin, a peer-to-peer electronic cash system. Unlike traditional currencies, which are issued by central banks, Bitcoin has no central authority [15]. Bitcoin is the first cryptocurrency that allows to perform transactions in a secure manner without the need of a trusted third-party, while also solving the double-spending problem. Nevertheless, Bitcoin was just the first of many Blockchain applications [52].
In a nutshell, Blockchain is a synchronized, shared, distributed, append-only database (ledger), that relies on strong consensus algorithms, such as Proof of Work and Proof of Stake, to maintain the peer-to-peer network [15]. Rather than being an entirely new technology, Blockchain is a combination of multiple existing technologies, mainly asymmetric key encryption, hash functions, Merkle trees, and peer-to-peer networks.
The information in Blockchain is stored in blocks that are linked together to form a chain [15]. Blocks consist of two types of data, a block header that contains metadata about the block, and the block content that contains the block's information, for instance a list of the block's transactions. The block's header is composed of

the hash root (hash digest of the block's data), the hash value of the previous block (except the genesis block), and a timestamp [15]. Since each block holds the hash value of the previous block, the blocks are cryptographically linked together after undergoing a validation process. As new blocks are added to the Blockchain, older blocks become more difficult to modify. This approach renders the Blockchain tamper-evident and tamper-resistant, lending to the key attribute of immutability [15, 52].

As a distributed ledger technology, Blockchain is managed by a peer-to-peer network. In this way, the digital ledger is shared, updated, and replicated within the network, and any conflicts are resolved automatically using established rules [15, 52].

Blockchain networks can be categorized based on their permission model. In Permissionless Blockchains, anyone can maintain the network by publishing blocks and participating in the consensus, as in the case of Permissioned Blockchains only particular users are allowed to do it [52]. There are four main types of Blockchain network architectures: Public, Private, Hybrid, and Consortium Blockchains. Public permissionless Blockchains are open for access to anyone and all users can publish and validate blocks without permission from any authority [52]. Private permissioned Blockchains are closed networks, usually owned by an entity or organisation, where only authorized users can participate in the network and perform operations over the distributed ledger. Hybrid Blockchains are a combination of Public and Private Blockchains that allow to control who can access specific information stored on chain and what information will be public. Finally, Consortium Blockchains, also known as Federated Blockchains, are similar to Hybrid Blockchains but instead of being managed by a single entity or organisation, they are managed by a group of organisations and individuals, typically referred to as a consortium [52].

3.2 General Data Protection Regulation

The General Data Protection Regulation (GDPR), which entered into force on 25 May 2018 [30, 39], is a legal regulation containing a set of measures designed to enhance privacy and privacy awareness in the European Union (EU) [43, 45]. The regulation is described in detail across 99 articles and applies to any entity or organization that processes personal data of EU citizens, regardless of where the data is processed [1]. By appointing higher requirements and obligations on entities who manage and process personal data, the GDPR aims to empower individuals with more control over their personal data [13, 17, 32, 40, 41, 45, 48].

According to Article 4 of the GDPR, "personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors", i.e., personal data is any information that can, directly or indirectly, be associated with a natural person.

The GDPR clearly differentiates three roles and specifies their associated rights and obligations under the EU law [45]. Data Subject is an identified or identifiable natural person whose personal data refers to. Data Controller is defined as "the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data". On the other hand, Data Processor is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Article 4 of the GDPR).

The means by which personal data should be protected are defined in the GDPR on a set of core data processing principles: Lawfulness, Fairness, and Transparency. Data subjects should be aware of the processing purposes and provided with proper notification and information regarding its scope; Purpose Limitation. Personal data should be used for specific and well-defined purposes; Data Minimization. Personal data should only be collected for processing purposes and redundant data should not be collected; Storage Limitation. Personal data should be stored no longer than necessary; Accuracy of data records; Integrity; and Confidentiality [45, 47].

Furthermore, the GDPR lays out a variety of rights aiming at providing the Data Subjects with more control over their personal data [1, 45], primarily the right to be informed (Article 13), right of access (Article 15), right to rectification (Article 16), right to erasure (Article 17), and right to data portability (Article 20).

3.3 Electronic Health Records

According to ISO/TR 14639, the electronic health record (EHR) is "information relevant to the wellness, health, and healthcare of an individual, in computer processable form and represented according to a standardized information model". EHRs is a digital collection of patients' medical data [25]. EHRs store a patient's demographics, medical history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results [6]. EHRs are operated by healthcare organizations and data are entered by physicians. Patients cannot access or control their own medical records. Its purpose is to collect data from healthcare professionals and facilitate electronic collaboration and information sharing between healthcare organizations, whereas patients are merely passive actors [6].

EHRs enable the integration of data between healthcare providers, facilitate and increase access to patients' data, reduce medical errors and their associated costs and losses, and consequently improve disease management quality of care [6]. However, the main limitation of EHR systems is related to interoperability [6].

3.4 Personal Health Records

Personal health records (PHRs) are a form of electronic health records (EHRs) [10]. Unlike EHRs, PHRs allow patients to manage and access their own medical data [6, 10, 19, 25, 38]. The fact that the patient is responsible for maintaining the data is seen as a key advantage over the EHR [6]. Also, PHRs allow to integrate data about a patient's lifestyle and wellness, as well as data withdrawn from various sensors that monitor their health state [6]. In sum, PHRs' provide a comprehensive overview of the patient's medical history, containing data entered by the patient,

lab results, as well as data from devices such as wearables sensors or collected from a smartphone [6, 25, 38]. Benefits of PHR include patient empowerment leading to improved outcomes and reduced healthcare costs [10].

4 Implementing GDPR-compliant Blockchain Solutions: A Systematic Literature Review

The SLR revealed that there is a growing interest in the use of Blockchain for personal data storing and processing purposes. Its distributed and immutable nature allows it to be applied to a wide variety of areas, including finance, healthcare, or to connected environments, such as the Internet of Things (IoT) ecosystem. Indeed, healthcare is one of the most addressed fields among the reviewed papers, where the application of Blockchain technology can enable transparent and fast access to personal healthcare data, promote data standardization, and enhance transfer and sharing of healthcare data [26].

Although Blockchain is regarded as a promising technology for areas that deal with sensitive information, its implementation raises a significant amount of challenges. The majority of reviewed papers identified the benefits and challenges of using Blockchain solutions for storing personal data, while others simply reported having developed and implemented a specific Blockchain solution.

On the one hand, a great deal of studies concludes that using Blockchain solutions for storing personal data has clear advantages compared to other conventional methods of storing information due to its privacy and security features. On the other hand, the use of Blockchain introduces some concerns, mainly compliance with legal regulations, privacy issues, and scalability limitations.

As privacy became a substantial public concern, it is crucial that privacy regulations, such as the GDPR, are considered when designing new applications. The GDPR, however, did not take emerging decentralized technologies into account during its development [1], which resulted in tension between Blockchain technology and the regulation [11]. The literature identifies the conflicts between Blockchain's immutable records and the GDPR's right to rectification (Article 16) and right to erasure (Article 17) as the most alarming concerns when developing Blockchain applications. Although deemed by many authors as its core value proposition, this immutability presents disadvantages for Blockchain technology when used in areas where the modification and deletion of data is demanded, and it is the reason several sectors are yet to completely embrace this new technology [23]. It is important to notice, however, that even though it is very difficult to amend blockchains, it is not impossible [11]. Other important challenges comprise the anonymization of personal data and the identification of the data controller and data processors. The latter is especially worrisome when dealing with public Blockchains [44].

The Blockchain technology, by design, cannot comply with legal regulations, such as the GDPR. However, this does not mean it cannot be compliant, it just implies the need to complement Blockchain with other technologies. The general consensus among the reviewed papers is to leverage off-chain storage capabilities in order to achieve compliance. In this solution, data classified as personal data is encrypted and stored off-chain, and is linked to the distributed ledger through a hash pointer. This solves several of the aforementioned challenges since the off-chain data can be modified or deleted at any time. Additionally, storing personal data off-chain improves scalability, reduces data storage requirements, and enhances privacy (Miyachi & Mackey, 2021). Other solutions include destroying the encryption key and the use of chameleon hash functions. The former lies in the premise that the GDPR does not "specify what constitutes erasure" since, technically, the data is not erased but rather deemed inaccessible, remaining stored in the Blockchain. The latter only works in private Blockchains and requires a trusted authority to hold the secret key, which defeats the purpose of blockchain to eliminate the need for third parties and centralized authority [1].

It is essential to mention that each of the presented solutions has its own limitations and should be chosen based on the specific use case. In fact, the compliance with GDPR will depend on the specific architecture that underlies a particular Blockchain application, each application must be evaluated independently, on a case-by-case basis.

Some studies proposed a set of good practices and guidelines for developers and architects to achieve GDPR compliance when building Blockchain solutions. An appropriate understanding of the GDPR principles and objectives is fundamental so that the Blockchain can be designed and tailored according to the GDPR requirements [43]. Furthermore, the principles of privacy-by-design and privacy-by-default, data minimization, transparency, pseudonymization, encryption and other privacy-enhancing tools should be applied when designing Blockchain applications. Smart contracts containing the users' consent should be implemented.

In short, Blockchain technology is an interesting alternative to traditional methods of storing information, however, the proper precautions should be taken and the foregoing challenges considered when implementing Blockchain applications.

5 Implications of the GDPR in Healthcare: A Systematic Literature Review

The papers reviewed in the SLR emphasised the importance of being compliant with GDPR, especially in an industry such as healthcare which deals with extremely sensitive personal data of patients. The lack of compliance may result in unnecessary risks to the rights and freedoms of individuals as well as organisations which may suffer from financial penalties for failing to comply with the regulations [9].

Even though it is mandatory for all EU member states, some papers acknowledged the benefits of being compliant with the GDPR in the healthcare industry. The literature identified the improved control of data subjects over their personal health data as one of the main benefits of compliance. By defining a variety of legal rights and imposing several requirements on data controllers and processors, the GDPR enables the data subjects to manage their personal health data however they see fit [9, 14, 16,

29, 31], except in specific cases such as in cases of public interest. This enhanced control leads to yet another benefit as it is one of the factors that positively influence the level of confidence data subjects have in the organisations that handle their personal data [2, 14]. Trust is key as it is what motivates individuals to share their personal data with the organisations. The standardization of data protection laws within the EU is also recognised as an advantage. However, it is important to note that, even though it is an improvement over the previous regulation, the manoeuvrability that the GDPR provides for further legislation at the national level, particularly in relation to exemptions, leads to some legal variances hindering the sharing of data [28].

Most articles focused on the challenges regarding compliance with the GDPR on healthcare as well as the requirements and obligations imposed on data controllers and processors. The literature considers achieving patients' consent one of the most disturbing concerns as the GDPR's stricter requirements add significant complexity to the use of patients' data [8]. The regulation, however, acknowledges the difficulty of obtaining specific and granular consent, particularly for scientific research, and so it recognises to some extent 'broad consent' (Recital 33). It is often not possible to fully identify the purpose of personal data processing at the time of data collection. Therefore, data subjects should be allowed to give their consent to only certain areas [7, 49]. Moreover, it is vital to understand that the notion of "consent" is different under the GDPR as opposed to the ones traditionally sought in clinical or scientific research. The standard notion of consent seeks a subject's free and voluntary expression of his or her willingness to participate in a particular clinical or scientific research, setting aside the duty of confidence. On the other hand, GDPR seeks consent for the processing of personal data. This implies a requirement for distinct formal processing for both types of consent [35]. [7] states that organisations may rely on consent to set aside the duty of confidence but rely on a different legal ground under the GDPR, namely the public interest and the research condition.

Several studies have also addressed the specific derogations for data concerning health laid out by the GDPR. The GDPR recognises the importance of science and innovation and is designed to facilitate the free flow of information. To that end, it defines several exemptions for processing of special categories of personal data, such as health data [20], which is prohibited under the GDPR. These can be observed in *section 6.3*. While explicit consent is considered the most common legal ground for processing, it is important to stress out that is not a mandatory requirement to comply with the GDPR [20].

This SLR has brought important contributions to both academia and industry on the effects of the GDPR on healthcare. At a time where huge amounts of personal health data are being generated daily due to the increasingly use of modern technologies, researchers, practitioners, healthcare organisations and other institutions that process or intend to process health data of individuals may resort to our study to gain awareness and to better understand their obligations under the GDPR and the procedures that they need to take to accomplish them. The quality of the evidence included in the review is considered to be high since the vast majority of the reviewed papers were published in top-tier scientific journals.

6 Blockchain for Health Tourism: A Multivocal Literature Review

The MLR revealed that there is a growing interest in recent years on the use of Blockchain technology to address and solve several of the challenges and inefficiencies inherent to the health tourism industry [3, 36, 42]. Nevertheless, blockchain technology is under constant development and its implementation in health tourism is still at an early stage, which reflects on the current literature being largely limited and fragmented [3]. The majority of the analysed studies that specifically address health tourism mostly focuses on raising awareness about the opportunities and applications for using blockchain in health tourism.

As mentioned in the literature, the use of blockchain allows for disintermediation, interoperability, trust and transparency. However, the technology has limitations that must be considered when applied in the health tourism sector.

One of the main limitations is related to data storage and management. The data integrity feature of the blockchain results in immutability, so any data that is entered into the blockchain cannot be deleted or changed. However, because health data is protected by privacy laws, it must be deleted if requested by a health tourist. In addition, although blockchain can perfectly be used as a database to record health data, it is not suitable for storing large volumes of data or high-speed data due to redundancy from many processing nodes holding a full copy of all data. To get around this limitation, only a hash or other metadata can be stored on the blockchain, while the key data is stored off-chain.

Another limitation of blockchain usage is the lack of standardization of blockchain architectures. This can hinder the establishment of relationships between healthcare providers implementing blockchain due to difficulties in integrating different architectures.

The most frequent implementations found in the literature consisted of distributed PHR systems leveraging both on-chain and off-chain capabilities where patients manage their own health records and decide who has access to their data. Though, it important to note that many of these solutions were not specifically designed for health tourism.

This MLR has brought important contributions to both academia and industry on the current state-of-the-art in the use of Blockchain for health tourism. At a time where huge amounts of personal health data are being generated and global healthcare is becoming more of a reality, researchers, practitioners, healthcare organisations and other institutions may resort to our study to gain awareness and to better understand the impact and relevance of the use of blockchain for health tourism practice.

Conclusion

Based on the knowledge gathered from the literature reviews, we developed a blockchain-based framework for healthcare data management that follows the GDPR, focused on the specific case of health tourism practice.

To ascertain the feasibility of using Blockchain technology to store personal data while being compliant with the GDPR, a Systematic Literature Review (SLR) was carried out to identify the benefits and challenges of using Blockchain technology to store personal data, and review the current state-of-the-art for implementing GDPR-compliant Blockchain solutions. The search produced a total of 432 candidate studies, including duplicates, from which 35 were deemed relevant to the SLR and read in full.

To assess the impact of the General Data Protection Regulation (GDPR) in the healthcare, a Systematic Literature Review (SLR) was carried out to identify the main benefits and challenges of compliance with the GDPR in the healthcare sector, as well as existing derogations from the regulation. The search produced a total of 589 candidate studies, including duplicates, from which 25 were deemed relevant to the SLR and read in full.

To investigate the current developments and perspectives on the use of Blockchain for the practice of health tourism, a Multivocal Literature Review (MLR) was carried out to identify and review existing evidence on both the state-of-the-art and practice on the use of blockchain solutions for health tourism. The search produced a total of 440 candidate studies, including duplicates, from which 27 were deemed relevant to the MLR and read in full.

Blockchain technology constitutes an exciting new alternative to traditional methods of storing and sharing information. Its distributed and immutable nature enables it to be applied to a wide variety of areas, including healthcare. It can address and solve many of the challenges and inefficiencies inherent to the health tourism industry [3, 36, 42]. Even so, the technology possesses certain limitations and its implementation raises a significant amount of challenges that must be considered when applied in the health tourism sector, mostly concerning compliance with legal regulations.

In a time where Blockchain is at an early stage of development and the practical implications of the GDPR on the technology are yet to be fully understood, researchers and practitioners may resort to our framework to gain awareness of the existing tensions and to better understand the impact and relevance of the GDPR on the development of Blockchain applications for health tourism.

Future Work

Future research is needed to study in detail the implications of the GDPR on the different types and specific domains of Blockchains. The regulation leaves room to modify certain aspects of the GDPR in specific EU member states data protection laws, so it is necessary to assess the implications of the GDPR on healthcare in specific EU member states, as well as the implications within the different areas of practice that comprise the healthcare sector.

Although the literature identifies off-chain storage as the best approach for achieving compliance, the solution is not unanimous among all the reviewed papers, hence, a generic solution for storing personal data on Blockchain is also indispensable.

Existing and upcoming Blockchain applications should be developed with conscious awareness of the tensions and challenges mentioned in this study and focus on the commonalities between Blockchain technology and the GDPR since, in the end, both are attempting to achieve the same objectives: enhance privacy and security, and increase the users' control over their personal data.

There is a need for clarification regarding some of the principles and requirements of the GDPR, for instance the meaning of "erasure", and the introduction of new and up-to-date regulations that take emerging decentralized technologies into consideration, which will most likely guide the development of the technology and increase its adoption.

Since blockchain technology is under constant development and its full impact on health tourism practice is yet to be fully understood further research on the topic is also needed. Additionally, it is of essence to consider the implication of data protection regulations, such as GDPR, in the implementation of blockchain systems in the health tourism industry.

With the knowledge gathered from this study, it would be interesting to develop a GDPR-compliant blockchain architecture for health tourism.

REFERENCES

[1] Al-Abdullah, M. et al. 2020. Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR. *Digital Policy, Regulation and Governance* . 22, 5–6 (Dec. 2020), 389–411. DOI: https://doi.org/10.1108/DPRG-04-2020-0050.

[2] Astrup, J. 2018. GDPR - THE TRANSFER OF DATA POWER. (2018).

[3] Balasubramanian, S. et al. 2022. Leveraging Blockchain in Medical Tourism Value Chain. *Information and Communication Technologies in Tourism 2022*. (2022), 78–83. DOI: https://doi.org/10.1007/978-3-030-94751-4_8.

[4] Bernal Bernabe, J. et al. 2019. Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*. Institute of Electrical and Electronics Engineers Inc.

[5] Campanile, L. et al. 2021. Designing a GDPR compliant blockchain-based IoV distributed information tracking system. *Information Processing and Management*. 58, 3 (May 2021). DOI: https://doi.org/10.1016/j.ipm.2021.102511.

[6] Cernian, A. et al. 2020. Patientdatachain: A blockchain-based approach to integrate personal health records. *Sensors (Switzerland)*. 20, 22 (Nov. 2020), 1–24. DOI: https://doi.org/10.3390/s20226538.

[7] Chico, V. 2018. The impact of the general data protection regulation on health research. *British Medical Bulletin*. 128, 1 (Dec. 2018), 109–118. DOI: https://doi.org/10.1093/bmb/ldy038.

[8] Crowhurst, N. et al. 2019. Implications for nursing and healthcare research of the general data protection regulation and retrospective reviews of patients' data. (2019).

[9] European Society of Radiology (ESR) 2017. The new EU General Data Protection Regulation: what the radiologist should know. *Insights into Imaging*. 8, 3 (Jun. 2017), 295–299. DOI: https://doi.org/10.1007/s13244-017-0552-7.

[10] Fang, H.S.A. et al. 2021. Blockchain personal health records: Systematic review. *Journal of Medical Internet Research*. 23, 4 (Apr. 2021). DOI: https://doi.org/10.2196/25094.

[11] Finck, M. 2018. Blockchains and Data Protection in the European Union. *European Data Protection Law Review*. 4, 1 (Mar. 2018), 17–35. DOI: https://doi.org/10.21552/edpl/2018/1/6.

[12] Garousi, V. et al. 2019. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*. 106, (Feb. 2019), 101–121. DOI: https://doi.org/10.1016/j.infsof.2018.09.006.

[13] Georgiou, D. and Lambrinoudakis, C. 2020. Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR). *Information (Switzerland)*. 11, 12 (Dec. 2020), 1–19. DOI: https://doi.org/10.3390/info11120586.

[14] Georgiou, D. and Lambrinoudakis, C. 2020. Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR). *Information (Switzerland)*. 11, 12 (Dec. 2020), 1–19. DOI: https://doi.org/10.3390/info11120586.

[15] Gupta, M. 2017. *Blockchain IBM Limited Edition*.

[16] Jekova, V. 2021. EU REQUIREMENTS FOR PROTECTION OF PERSONAL DATA OF PATIENTS IN HEALTH ESTABLISHMENTS. *KNOWLEDGE-International Journal*. 46, 5 (2021).

[17] Jekova, V. *EU REQUIREMENTS FOR PROTECTION OF PERSONAL DATA OF PATIENTS IN HEALTH ESTABLISHMENTS.*

[18] Junejo, A.Z. et al. 2021. Blockchain Privacy Preservation by Limiting Verifying Nodes' during Transaction Broadcasting. *3rd International Conference on Electrical, Communication and Computer Engineering, ICECCE 2021* (Jun. 2021).

[19] Kim, J.W. et al. 2022. A Blockchain-Applied Personal Health Record Application: Development and User Experience. *Applied Sciences (Switzerland)*. 12, 4 (Feb. 2022). DOI: https://doi.org/10.3390/app12041847.

[20] Kirwan, M. et al. 2020. What GDPR and the Health Research Regulations (HRRs) mean for Ireland: "explicit consent"—a legal analysis. *Irish Journal of Medical Sciences*. (2020). DOI: https://doi.org/10.1007/s11845-020-02331-2/Published.

[21] Kitchenham, B. 2004. *Procedures for Performing Systematic Reviews*.

[22] Kitchenham, B. and Charters, S. 2007. *Guidelines for performing Systematic Literature Reviews in Software Engineering*.

[23] Lee, N.Y. et al. 2019. Modifiable Public Blockchains Using Truncated Hashing and Sidechains. *IEEE Access*. 7, (2019), 173571–173582. DOI: https://doi.org/10.1109/ACCESS.2019.2956628.

[24] Liu, L. and Xu, B. 2018. Research on Information Security Technology Based on Blockchain. (2018).

[25] Madine, M.M. et al. 2020. Blockchain for Giving Patients Control over Their Medical Records. *IEEE Access*. 8, (2020), 193102–193115. DOI: https://doi.org/10.1109/ACCESS.2020.3032553.

[26] Miyachi, K. and Mackey, T.K. 2021. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information Processing and Management*. 58, 3 (May 2021). DOI: https://doi.org/10.1016/j.ipm.2021.102535.

[27] Mocydlarz-Adamcewicz, M. 2021. Effective communication between hospital staff and patients in compliance with personal data protection regulations. *Reports of Practical Oncology and Radiotherapy*. 26, 6 (2021), 833–838. DOI: https://doi.org/10.5603/RPOR.a2021.0138.

[28] Molnár-Gábor, F. et al. 2021. Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden. *Seminars in Cancer Biology*. (2021). DOI: https://doi.org/10.1016/j.semcancer.2021.12.001.

[29] Muchagata, J. and Ferreira, A. 2018. Translating GDPR into the mHealth Practice. (2018).

[30] Mulder, T. 2019. Health Apps, their Privacy Policies and the GDPR. (2019).

[31] Mustafa, U. and Philip, N. 2019. A Novel Privacy Framework for Secure M-health Applications: The Case of the GDPR. (2019).

[32] Mustafa, U. and Philip, N. *A Novel Privacy Framework for Secure M-health Applications: The Case of the GDPR.*

[33] Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. (2008).

[34] Parekh, J. et al. 2021. Disintermediation in medical tourism through blockchain technology: an analysis using value-focused thinking approach. *Information Technology and Tourism*. 23, 1 (Mar. 2021), 69–96. DOI: https://doi.org/10.1007/s40558-020-00180-4.

[35] Rajam, N. 2020. Policy strategies for personalising medicine "in the data moment." *Health Policy and Technology*. 9, 3 (Sep. 2020), 379–383. DOI: https://doi.org/10.1016/j.hlpt.2020.07.003.

[36] Rejeb, A. et al. 2019. The Impact of Blockchain on Medical Tourism. *WeB2019 Workshop on e-Business*. (2019).

[37] Riva, G.M. 2020. What Happens in Blockchain Stays in Blockchain. A Legal Solution to Conflicts Between Digital Ledgers and Privacy Rights. *Frontiers in Blockchain*. 3, (Aug. 2020). DOI: https://doi.org/10.3389/fbloc.2020.00036.

[38] Salonikias, S. et al. 2022. Blockchain-Based Access Control in a Globalized Healthcare Provisioning Ecosystem. *Electronics (Switzerland)*. 11, 17 (Sep. 2022). DOI: https://doi.org/10.3390/electronics11172652.

[39] Shah, S.M. and Khan, R.A. 2020. Secondary use of electronic health record: Opportunities and challenges. *IEEE Access*. 8, (2020), 136947–136965. DOI: https://doi.org/10.1109/ACCESS.2020.3011099.

[40] Shu, I.N. and Jahankhani, H. 2017. The Impact of the new European General Data Protection Regulation (GDPR) on the Information Governance Toolkit in Health and Social Care with Special Reference to Primary Care in England. *Proceedings - 2017 Cybersecurity and Cyberforensics Conference, CCC 2017* (Jul. 2017), 31–37.

[41] Sousa, M. et al. 2018. OpenEHR based systems and the general data protection regulation (GDPR). *Studies in Health Technology and Informatics* (2018), 91–95.

[42] Stephano, R.-M. 2019. Blockchain Technology: A Total Game-Changer in Medical Tourism. *Medical Tourism Magazine*.

[43] Tatar, U. et al. 2020. Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law and Security Review*. 38, (Sep. 2020). DOI: https://doi.org/10.1016/j.clsr.2020.105454.

[44] Teperdjian, R. 2020. THE PUZZLE OF SQUARING BLOCKCHAIN WITH THE GENERAL DATA PROTECTION REGULATION. 60, 3 (2020).

[45] Truong, N.B. et al. 2020. GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security*. 15, (2020), 1746–1761. DOI: https://doi.org/10.1109/TIFS.2019.2948287.

[46] Tyan, I. et al. 2021. The benefits of blockchain technology for medical tourism. *Sustainability (Switzerland)*. 13, 22 (Nov. 2021). DOI: https://doi.org/10.3390/su132212448.

[47] Vasylkovskyi, V. et al. 2020. BlockRobot: Increasing Privacy in Human Robot Interaction by Using Blockchain. *Proceedings - 2020 IEEE International Conference on Blockchain, Blockchain 2020* (Nov. 2020), 106–115.

[48] van Veen, E. ben 2018. Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate. *European Journal of Cancer*. 104, (Nov. 2018), 70–80. DOI: https://doi.org/10.1016/j.ejca.2018.09.032.

[49] van Veen, E. ben 2018. Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate. *European Journal of Cancer*. 104, (Nov. 2018), 70–80. DOI: https://doi.org/10.1016/j.ejca.2018.09.032.

[50] Webster, J. and Watson, R.T. 2002. *ANALYZING THE PAST TO PREPARE FOR THE FUTURE: WRITING A LITERATURE REVIEW*.

[51] Wierda, E. et al. 2018. Privacy of patient data in quality-of-care registries in cardiology and cardiothoracic surgery: The impact of the new general data protection regulation EU-law. *European Heart Journal - Quality of Care and Clinical Outcomes*. 4, 4 (Oct. 2018), 239–245. DOI: https://doi.org/10.1093/ehjqcco/qcy034.

[52] Yaga, D. et al. 2018. Blockchain Technology Overview. (Jun. 2018). DOI: https://doi.org/10.6028/NIST.IR.8202.