GDPR COMPLIANCE FOR BLOCKCHAIN APPLICATIONS IN HEALTHCARE

Anton Hasselgren[1], Paul Kengfai Wan[2], Margareth Horn[3], Katina Kralevska[4], Danilo Gligoroski[4] and Arild Faxvaag[1]

[1]Department of Neuromedicine and Movement Science, NTNU, Norwegian University of Science and Technology, Trondheim, Norway
[2]Department of Manufacturing and Civil engineering, NTNU, Norwegian University of Science and Technology, Trondheim, Norway
[3]Department of Sociology and Political Science, NTNU, Norwegian University of Science and Technology, Trondheim, Norway
[4]Department of Information Security and Communication Technology, NTNU, Norwegian University of Science and Technology, Trondheim, Norway

ABSTRACT

The transparent and decentralized characteristics associated with blockchain can be both appealing and problematic when applied to a healthcare use-case. As health data is highly sensitive, it is therefore, highly regulated to ensure the privacy of patients. At the same time, access to health data and interoperability are in high demand. Regulatory frameworks such as GDPR and HIPAA are, amongst other objectives, meant to contribute to mitigating the risk of privacy violations of health data. Blockchain features can likely improve interoperability and access control to health data, and at the same time, preserve or even increase, the privacy of patients. Blockchain applications should address compliance with the current regulatory framework to increase real-world feasibility. This exploratory work indicates that published proof-of-concepts in the healthcare domain comply with GDPR, to an extent. Blockchain developers need to make design choices to be compliant with GDPR since currently, none available blockchain platform can show compliance out of the box.

KEYWORDS

Blockchain, DTL, health data, GDPR, privacy regulations

1. INTRODUCTION

The current status in data privacy could be categorized as the post-privacy area due to the unintended consequences of the big data revolution. The famous Cambridge Analytica scandal [1] is an example of how re-identification can be achieved by cross-analysing large data sets containing private information. The technology revolution that has driven us to post-privacy has not been stopped through privacy acts such as General Data Protection Regulation (GDPR). At the same time, we are currently in another (r)evolution that can restore data privacy - blockchain.

In 2018, The European Union instituted the GDPR [2], which regulates the collection, processing and securing of personal data, including protected health information (PHI). Art. 4(15) of the EU GDPR, defines data concerning health as: “personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status.”

David C. Wyld et al. (Eds): BIBC, AISO, EDTECH - 2020
pp. 23-35, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101303

Health Insurance Portability and Accountability Act (HIPPA) is essential for U.S. healthcare law and deals mainly with privacy rights and access rather than ownership of patient data [3]. Each state has ownership of patient data of its citizens, and in this case, it is controlled by respective state law. Since there are 50 states, there are 50 differing laws, court cases and interpretations of that ownership of patient data. New Hampshire is the only state which enacted the legislation stating that the ownership of health data lies with the patient. How GDPR will interact and comply with U.S. state laws remains to be determined. HIPPA is an important regulatory framework but the scope of this work only covers GDPR compliance.

Blockchain, first introduced with the launch of Bitcoin back in 2008, has become more diluted in its definition. Currently, there is no fixed or a widely accepted definition of the term blockchain. To clarify its use in this research, we have defined blockchain as a distributed, decentralized and tamper-proof ledger without any centralized control. Blockchain technology and other Distributed Ledger Technologies (DLT) could increase our data privacy and empower individuals with control and access over their data, including health data. The objective of this study is twofold: (i) to dissect the various designs of blockchain and explore GDPR compliance for different components in established or proposed blockchain applications in the healthcare sector and, (ii) to provide a future researcher with guidance in how to comply with GDPR when designing blockchain application within the healthcare domain.

The rest of this paper is organized as follows: Section 2 provides a brief introduction to blockchain technology and outlines previous work addressing blockchain compliance with GDPR; Section 3 presents the research approach; Section 4 describes four blockchain applications in healthcare identified through the literature; Section 5presents our results and analysis; Section 6 provides a discussion and conclusion to the work, and givesrecommendations for future work.

2. GDPR AND BLOCKCHAIN

This section gives a brief introduction to blockchain and GDPR. We can broadly categorize blockchain as; public permissionless, private permissioned and federated permissioned. The categorization is important in order to design applications in relevant sectors to achieve social and economic goals. In a public blockchain, everyone in the network holds equal rights and the ability to access the ledger. While nodes need to be certified to join the consensus process in private and federated blockchains, which makes them permissioned. The French National Commission on Informatics and Liberty (CNIL) recommends private permissioned blockchains because of the possible compliance with GDPR [4]. The third blockchain category is a combination between public and private, which are referred to as a federated or hybrid blockchain [5].

Previous research has explored blockchain platforms and their feasibility for healthcare [6] and concluded that none of the most widely used blockchain platforms were ideal for healthcare, out of the box. Other work has identified important properties and characteristics in different types of blockchain, and they need to be considered in the initial design phase; identity management, efficiency according to energy use, immutability, ownership management and transaction approval [5]. Public, private and federated blockchains handle these properties differently and each component may have their limitation [7].

As detailed by the European Union Blockchain Observatory and Forum [4], in principle, there are no contradictions between the goals of GDPR and DLT. However, there seem to be at least three areas in which GDPR still does not offer enough clarity about how real-world DLT applications for the health sector should be developed: (1) accountability and roles (e.g., how to identify a data controller in a public DLT), (2) anonymization of personal data (e.g., which techniques are sufficient to anonymize personal data to the point where the resulting output can potentially be stored in a DLT), and (3) GDPR rights conflicts (e.g., how to rectify or remove personal data that are recorded in a DLT that is immutable by nature, or who is responsible for requesting and managing the “freely, specific, informed, and unambiguous” consent from a data subject, especially if the data controller is not specified) [8]. With regards to the anonymization of personal data, it is clear that GDPR does not apply to anonymized data and thus, this type of information can be stored on the open ledger. However, what qualifies as anonymized data is still unclear. The only indication today is that it must be irreversibly impossible to identify an individual through any of the means “reasonably” likely to be used [9].

Smart contracts are one of the components that have been proposed on blockchain platforms to reduce the need for a third party. It enables a new type of autonomous regulation that executes transactions when all the requirements are fulfilled [10]. All legal rules and contracts are transposed into digital and software rules, which means that smart contracts can be the regulator in blockchain networks and rules are enforced accordingly [11]. For example, after a user authenticates its digital identity successfully, a smart contract can grant authorization and access to his/her medical records by the requestors [12]. However, Giordanengo at al. analysed some use cases of smart contracts and found out that none of the studies have reached the stage of production and concluded that it is not ready for implementation in the healthcare domain [13].

The design options in a blockchain application are wide, and there is an increase in both research and innovation. In order to design blockchain applications for healthcare use-cases, there are several important design choices the developer has to make, with the three most prominent: (1) choice of platform/network, (2) on/off chain data storage and (3) identity solution for interaction with the system.

2.1. Related Work

This section highlights previous work which has investigated blockchain compliance with GDPR. There is limited published research under this topic in the literature, but previous work has indicated the need for standardization [6] [7].

Two reports published by EU entities: The EU blockchain Observatory and Forum - Blockchain and the GDPR [4] and the European Parliamentary Research Service (EPRS) - Blockchain and the general data protection regulation [14] provide guidance in blockchain compliance with GDPR.

Blockchain and the GDPR is a thematic report published in 2018 where accountability and roles, as well as anonymization of personal data, are addressed. This report highlights the need for each blockchain use-case to be thoroughly analysed and rated in various interpretations - compliance with GDPR is not about the technology but rather, how it is utilized. The report also points out the need to avoid storing personal data on a public blockchain and anonymous data techniques such as obfuscation, encryption and aggregation should be used. The report proposed some principles to consider when designing blockchain architectures such as; considering user perspective, analysing where the personal data appears and who is responsible for the processing.

The Blockchain and the GDPR report have defined roles for three main actors: data subject, data controller and data processor, and outlined in the report that it can be problematic to identify the data controller in blockchain networks. The report also presents some techniques, such as reversible encryption and hashing, to achieve anonymous or pseudo-anonymous data. It is also important to consider if personal data should be involved when linking private chains with public chains.

In the report by the European Parliamentary Research Service, blockchain is defined as a combination of many different forms of distributed databases that present variation, both in complexity and governance agreement. The report gives an account of difficulties in whether personal data, can be anonymized to the extent that it meets the GDPR threshold of anonymization. Two types of compliance tension are expressed: (1) GDPR assumes that there is a data controller, which is often not the case in blockchains and (2) the right to be forgotten, which is problematic in an immutable ledger. Furthermore, it is expressed that it is difficult to assess the compatibility between blockchain and GDPR without having to pay attention to the nuances in blockchain configurations. There is also a request for further clarifications of concepts such as; ”anonymous data”, ”data controller” and the meaning of”erasure” under Art. 17.

There are some examples where blockchains and GDPR compliance are tested, such as the proof of-concept (PoC) developed for the use case of managing blood glucose data [26]. The concept provides a system for immutable, interoperable and GDPR compliant data exchange. In the PoC, it is highlighted that blockchain has a great potential to improve information transactions in a secure and transparent manner, between patients and providers [26]. Two tested solutions where explored, one based on the public IOTA blockchain and one in combination with public IOTA plus, a private IPFS (Inter Planetary File System) cluster. In the public IOTA it became difficult to eliminate the risk of personal data link ability and combining a public DLT and IPFS has a high degree of complexity. It is also highlighted that there are limitations in identifying a data controller since the public DLT ecosystem is formed by multiple healthcare stakeholders, as well as patient consent management. They argue that each use-case must be carefully considered when blockchain-based system is designed for health data exchange.

A private blockchain is suggested in the CUREX project, which is argued to be in GDPR compliance by design in a decentralized architecture [15]. In this project, it is argued that all data transactions in the health sector and their vulnerability are depend on a private blockchain infrastructure, to integrity of risk management. The CUREX project’s goal is to ensure the integrity of the risk assessment process of all data transactions.

Two other suggested GDPR-compliant design concepts address health data collected by sensors in different types of mobile and smart devices [16][17]. Both designs were described to address the vulnerability in centralised data storage controlled by service providers and ”the right to own and share personal information”. One of the concepts is combining blockchain with cloud storage and machine learning techniques to give users the possibility to share personal data easily and securely. In this model, the data is encrypted before uploaded to the cloud storage and secured by a hash function. The access to the data is distributed among multiple key keepers where no visible personal information is involved because the blockchain allows pseudonyms [16]. While the former considered the limits blockchain has to store large-size data that are continuous-dynamic, [17] propose architecture for efficient access and control mechanisms. In their work, the privacy challenge was addressed, and their design concept is an efficient privacy-preserving access to give the users full control over their own data.

3. METHOD

The research approach in this work has been: (i) review of four different blockchain proof-of concepts in health care; (ii) review of GDPR and how the regulations apply to health informatics; and (iii) an exploratory analysis on how the platforms reviewed in the review (i) comply with the relevant articles identified in GDPR (ii).

The blockchain based proof-of-concepts in (i) were identified through a scoping search in PubMed and Scopus.

The following documents were identified and utilized in (ii):

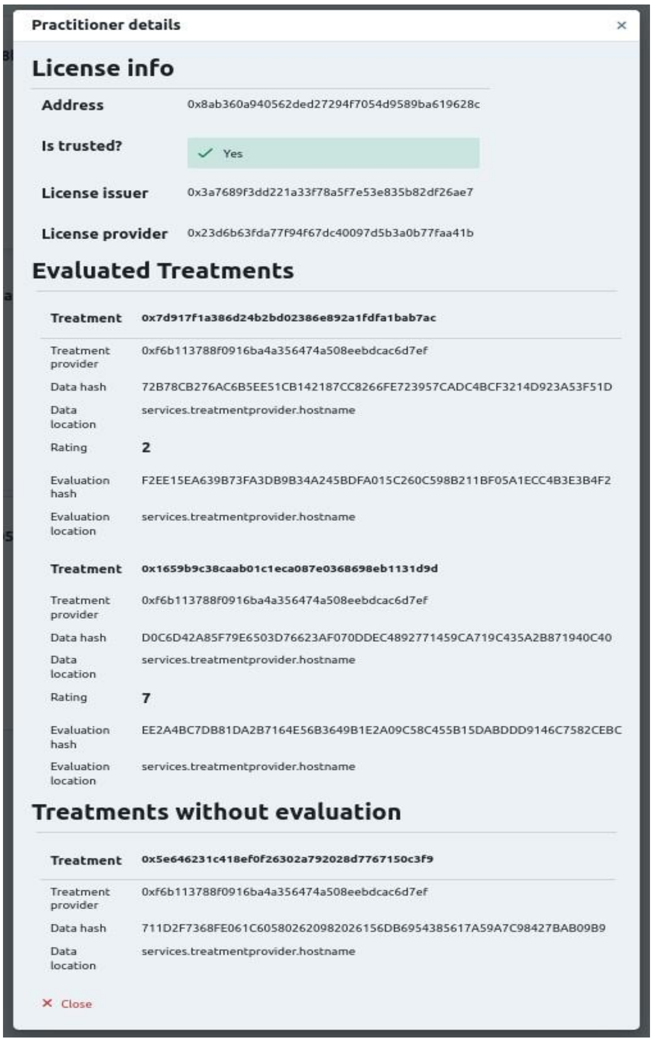
- GDPR (official document) [2];
- Blockchain and the General Data Protection Regulation [18].

4. BLOCKCHAIN-BASED HEALTHCARE APPLICATIONS

This section describes four different blockchain applications that were identified in a scoping search in PubMed and Scopus. These four applications were included based on their different architecture; the sample is not meant to be comprehensive. MedRec [19] is a blockchain- based solution for personal control of identity and the distribution of health information. The system is designed on the public Ethereum blockchain. This means that transactions, including metadata, which is sensitive in medical context, are visible to everyone who has access to the blockchain. And if someone can identify the patient's real-world identity and Ethereum account, one can determine the relationship between the health providers and the patients. In order to circumvent this privacy issue, MedRec anonymized metadata through disassociating each patient's identity from the provider, where each provider makes a new identity Ethereum account for each patient provider relationship. The purpose is to enable patients to establish public relations without revealing the real-world identities.

EMRshare [20] is a health data sharing application where different entities such as health provider, data scientists and patients interact using the permissioned Hyperledger blockchain. Transactions such as health data requests, approval or rejection action are stored on blockchain. While actual medical data are stored off-chain and encrypted with asymmetric encryption for security purposes. EMRshare also enables patients, the data owner, to anonymize their name or identity in the medical records before reaching the requestors.

VerifyMed [21][23] is a public Ethereum blockchain platform with the aim to validate the authorization and competence of healthcare workers in a virtualized healthcare environment. VerifyMed enables healthcare workers to document their work history and competence in the form of a de-centralized portfolio. VerifyMed combines and stores three forms of data items; evidence of authority, evidence of experience and evidence of competence to build their portfolios. Digital signatures scheme is also incorporated in VerifyMed to ensure ownership is established on each verified evidence. As an example of how a typical user interface looks like in a blockchain- based application, we give Figure 1, which is taken from VerifyMed [22], [23].



Practitioner details

License info

Address	0x8ab360a940562ded27294f7054d9589ba619628c
Is trusted?	✓ Yes
License issuer	0x3a7689f3dd221a33f78a5f7e53e835b82df26ae7
License provider	0x23d6b63fda77f94f67dc40097d5b3a0b77faa41b

Evaluated Treatments

Treatment	0x7d917f1a386d24b2bd02386e892a1fdfa1bab7ac
Treatment provider	0xf6b113788f0916ba4a356474a508eebdcac6d7ef
Data hash	72B78CB276AC6B5EE51CB142187CC8266FE723957CADC4BCF3214D923A53F51D
Data location	services.treatmentprovider.hostname
Rating	2
Evaluation hash	F2EE15EA639B73FA3DB9B34A245BDFA015C260C598B211BF05A1ECC4B3E3B4F2
Evaluation location	services.treatmentprovider.hostname
Treatment	0x1659b9c38caab01c1eca087e0368698eb1131d9d
Treatment provider	0xf6b113788f0916ba4a356474a508eebdcac6d7ef
Data hash	D0C6D42A85F79E6503D76623AF070DDEC4892771459CA719C435A2B871940C40
Data location	services.treatmentprovider.hostname
Rating	7
Evaluation hash	EE2A4BC7DB81DA2B7164E56B3649B1E2A09C58C455B15DABDDD9146C7582CEBC
Evaluation location	services.treatmentprovider.hostname

Treatments without evaluation

Treatment	0x5e646231c418ef0f26302a792028d7767150c3f9
Treatment provider	0xf6b113788f0916ba4a356474a508eebdcac6d7ef
Data hash	711D2F7368FE061C605802620982026156DB6954385617A59A7C98427BAB09B9
Data location	services.treatmentprovider.hostname

Figure 1. Page from the User Interface of VerifyMed for showing detailsabout all data related to a healthcare worker [22], [23]

FHIRChain [24] is a public Ethereum blockchain architecture for secure and scalable clinical data sharing with the goal to meet the requirements of The Office of the National Coordinator for the Health Information Technology (ONC) such as privacy preserving and health information security. FHIRChain stores encrypted metadata on the network rather than storing encrypted sensitive health data. It uses digital health identity, which utilizes public- key cryptography to generate and manage the identities. Often clinical data research data format and structures varies from institution to institution, which makes data sharing challenging, FHIRChain is developed based on HL7 Fast Healthcare Interoperability Resources (FHIR) to enforce consistent data formats for easier information sharing.

These proposed blockchain concepts within the healthcare domain primarily focus on solving interoperability without compromising the privacy and security of sensitive health data. Identity management for both patients and health workers are also considered as part of the proposed applications. However, the research work focusing on the degree of compliance to GDPR and other health data regulatory frameworks remains limited.

5. RESULTS

The results are presented mainly in Table 1 - relevance of GDPR for healthcare and analysis of compliance and Table 2 - Comparative analyses.

GDPR will have a significant impact on the healthcare sector in collecting, processing, and securing protected health information. Healthcare institutions (HI), are obligated to ensure that data is collected for a specific and legitimate use and only used for that purpose. Further, a healthcare organization will be required to obtain exclusive consent or permission from the patients (the data subject) to use their data according to (Art. 7).

GDPR indicates that the ownership of health data should be with the patients, enabling patients to have greater autonomy over their data. Healthcare providers are obligated to furnish patients with complete information when they request it, within specified time limits (Art. 15).

Additionally, GDPR requires organizations to report a data breach within 72 hours (Art. 33) and notify the affected individual (Art. 34). The onus will, therefore, be on healthcare organizations to ensure that data is highly secured and protected from unauthorized access or face rapid reporting requirements of breaches and possible severe financial penalties (see Art. 83). This is important when it comes to embracing new digital technologies like blockchain because issues such as misuse of patients' PHI would result in losing trust in healthcare institutions and delaying the adoption of blockchain in enhancing information sharing.

Table I summarizes what healthcare institutions (HI) must consider when using blockchain and DLT to secure and protect PHI and avoid costly fines for non-compliance.

Table 1. Relevance of GDPR for healthcare

Article in GDPR	Compliance	Impact in healthcare
Art. 30 (Records of processing activities), Art. 35 (Data protection impact assessment)	Able to conduct information audit to demonstrate GDPR compliance	HI is required to keep an up-to-date and detailed list of their processing activities using a data protection impact assessment. The list should include the purposes of the processing, what kind of data you process and who has access to it in the organization
Art. 6 (Lawfulness of processing), Art. 7 (Conditions for consent)	Legal justification for processing health data	HI can justify the purpose according to one of the six conditions. E.g Patients has given consent for the processing. Extra obligation such as the opportunity to revoke consent must be available to patients
Art. 12 (Transparent information, communication and modalities for the exerciseof the rights of the data subject)	Clear information about the data processing and legal justification in privacy policy	HI is obligated to inform patients that health data is collected. HI should explain why this is collected, how it is processed, who has the access and how it is secured using clear and plain language, particularly when addressing specifically to a child.
Art. 33 (Notification of apersonal data breach to the supervisory authority), Art. 34 GDPR (Communication of a personal data breach to the data subject)	Have a process to notify the authorities in the event of a data breach	HI is required to notify the supervisor authority in their jurisdiction within 72 hours learning of the health data breached or exposed. Patients should be notified without undue delay in plain language, if the breach is likely to put them at risk.

Art. 32 (Security of processing)	Encrypt, pseudonymize or anonymize personal data whenever possible	HI is to encrypt, pseudonymize or anonymize PHI whenever feasible.
Art. 25 (Data protection by design and by default), Art. 5 (Principles relating to processing of personal data)	Data protection is considered at all times, including at the beginning of developing aproduct	HI should implement appropriate technical (encryption) and organizational measures (deleting patient’s data that is no longer needed) to protect data. HI which adheres to data protection principles when processing of personal data is involved.
Art. 25 (Data protection by design and by default)	Designated person for ensuring GDPR compliance across the organization	HI should designate someone that is accountable for GDPR compliance which includes evaluation of data protection policies and the implementation of policies. HI should be able to verify the patient’s identity.
Art. 15 (Right of access by the data subject)	Able to verify the patients’ identity	HI is obligated to furnish patients with complete information when they request it and should be able to comply within a month. HI should be able to verify the patient’sidentity.
Art. 17 (Right to erasure/ ‘right to be forgotten’)	Easy to delete personal data upon request	Patients should have the right to request to delete all health data and HI should honor their request within a month. HI may have grounds to deny the request such as compliance with a legal obligation. HI should be able to verify the patient’s identity.
Art. 18 (Right to restriction of processing)	Easy to stop data processing upon request	Patients can request HI to restrict or stop processing their health data if certain grounds apply, such as dispute about the lawfulness of the processing. HI may be allowed to keep storing their data although the processing is restricted.
Art. 24 (Responsibility of the controller)	Establish the responsibility and liability of the controller	Any processing of personal data carried out by HI or on HI’s behalf, responsibilities should be established which includes implementing appropriate technical and organizational measures. This is to ensure and to be able to demonstrate that processing is performed lawfully
Art. 20 (Right to data portability)	Easy to receive a copy of your personal data and share with another in a simple format	From a privacy standpoint, GDPR offers higher patients’ autonomy over their data, instead of HI. This means patients should be able to receive health data in a readable format or share with other HI.

Blockchain structure can enhance the traceability of data making transactions auditable and transparent. In addition, storing data on the blockchain ledger could increase data integrity due to the inherited immutability property. However, any form of information stored on blockchain remains on blockchain which might violate GDPR since patients should have the right to erase their personal data. Although, it is common that national health data law prohibits the deletion of patient data from medical health records. Storing metadata could be an alternative to storing the full dataset. Storing metadata on the blockchain can pseudonymize a patient’s identity and to further protect patient’s identity, encryption technology such as zero-knowledge proofs could be implemented to prevent any forms of identification.

Table 2 presents a summary of how four different blockchain-based applications (presented under Section 4) comply with the relevant GDPR articles presented in Table 1.

Table 2. Comperative analysis

Features	**GDPR article**	**Blockchain application**			
		MedRec	EMRshare	FHIR chain	VerifyMed
Able to conduct information audit to demonstrate GDPR compliance	Art. 30 GDPR (Records of processing activities)	Yes	Yes	Yes	Yes
	Art. 35 GDPR (Data protection impact assessment)	N/A	N/A	N/A	N/A
Legal justification for processing health data	Art. 6 GDPR (Lawfulness of processing))	N/A	N/A	Yes	N/A
	Art. 7 GDPR (Conditions for consent)	N/A	Yes	Yes	N/A
Clear information about the data processing and legal justification in privacy policy	Art. 12 GDPR (Transparent information, communication and modalities for the exercise of the rights of the data subject)	Yes	Yes	Yes	Yes
Have a process to notify the authorities in the event of a data breach	Art. 33 GDPR (Notification of a personal data breach to the supervisory authority)	No	No	No	No
	Art. 34 GDPR (Communication of a personal data breach to the data subject)	No	No	No	No
Data protection is considered at all times, including at the beginning of developing a product	Art. 25 GDPR (Data protection by design and by default)	Yes	Yes	Yes	Yes
	Art. 5 GDPR (Principles relating to processing of personal data)	N/A	N/A	N/A	N/A
Encrypt, pseudonymize or anonymize personal data whenever possible	Art. 32 GDPR (Security of processing)	Yes	Yes	Yes	Yes
Designated person for ensuring GDPR compliance across the organization	Art. 25 GDPR (Data protection by design and by default)	No	No	No	No
Should be able to verify the patients identity.	Art. 15 GDPR (Right of access by the data subject)	Yes	Yes	Yes	No
Easy to delete personal data upon request	Art. 17 GDPR (Right to erasure/‘right to be forgotten’)	No	No	No	No
Easy to stop data processing upon request	Art. 18 GDPR (Right to restriction of processing)	N/A	No	N/A	No
Establish the responsibility and liability of the controller	Art. 24 GDPR (Responsibility of the controller)	No	No	No	No
Easy to receive a copy of your personal data and share with another in a simple format	Art. 20 GDPR (Right to data portability)	Yes	Yes	Yes	No

All four concepts use slightly different components of blockchain technologies. For example, FHIRchain uses a public blockchain (Ethereum) while EMRshare uses a permissioned blockchain (Hyperledger). These blockchains vary in some properties, such as the degree of visibility, but both types of blockchains can store transaction chronological with high data integrity due to the immutable structure. Blockchain data structure is easily auditable, which can make it inherited compliant with Art 30 and 35.

Identity management also forms a core technology in all these frameworks. This is one of the key compliances to Art 15. ”Right access by the right data”, before executing requests from patients to obtain health information or stop processing their health data. This is to prevent any misuse of private health data by the wrong person. For example, FHIRchain adopts digital identity to verify and authenticate the identity of clinicians. VerifyMed does not incorporate identity management to authenticate as the application utilizes evidence of authority to proof the credential of the clinicians.

Table 2 highlights that the blockchain concepts identified for this work did not fulfill the requirement of the right to forgetting (Art. 17). Patients can have the right to request for deletion of their information but the immutability nature of blockchain contradicts this article. To circumvent this, proposed concepts, such as FHIRchain, only stores metadata and protected with encryptions. Although it is not erasure, it prevents an unauthorized person from obtaining information and linking the pseudonymized metadata to patient’s identity. Currently, these four explored concepts did not state any procedures to notify authorities if any violation of GDPR is detected and might, therefore, lack compliance with (Art 33). A smart contract can be designed by sending a notification to relevant authorities when a breach is detected. In addition to that, a designated person for ensuring GDPR compliance within the network should be considered for future work.

6. DISCUSSION

There is an increased focus on blockchain technology in healthcare sector in both academic spheres and the private sector with the expectation that this technology could have a positive impact on achieving better interoperability and access to health data [25]. This can bring medical advances, such as enabling collaborative treatment and care decision. However, storing patient’s health data or even metadata is considered highly sensitive and could violate patient’s data privacy. In order to protect patient’s health data, GDPR has defined rules and guidelines to ensure that data processing and handling comply. However, research focusing on the degree of compliance of proposed blockchain solutions to GDPR in the healthcare sector remains limited.

The contribution of this paper explores how four different blockchain-based healthcare applications comply with the identified articles in GDPR. This analysis can provide further research guidance on how to achieve GDPR compliance and what architectural design choices that need to be considered.

As outlined under Section 5, compliance with Art 30 and 35 are achieved in the four healthcare applications identified due to the inherited characteristics of blockchain - storage of transaction chronological with high data integrity. Identity management is a core technology for healthcare applications, and it is also a key compliance factor in GDPR with Art 15: Right access by the right data. This is mainly to prevent any misuse of private health data by the wrong person and compliance is achieved with three out of the four concepts.

Currently, none of the proposed concepts fulfil the requirement of the right to be forgotten (Art 17), as shown in Table 2. This indicates that patients should have the right to request the deletion of their information. However, this is often regulated by national health data laws that prohibit the deletion of data from medical health records. Nevertheless, compliance with this article is problematic due to the immutable nature of blockchain. Compliance can be achieved by making all data stored on the ledger entirely anonymous or fully encrypted. Hence, we encourage researchers to explore full anonymity in blockchain applications for this domain.

None of the investigated blockchain concepts did consider the process of notifying authorities if any violation of GDPR is detected stated in Art. 33 as shown in Table 2. This could potentially be implemented by a smart contract to ensure automated and imitate notifications to relevant authorities upon data breach. A way to ensure that any new blockchain solutions that handle sensitive health data comply with GDPR, is to keep an up-to-date list using Data Protection Impact Assessment (DPIA) (Art. 35) to any authorities or regulators upon requests. This can avoid any solution providers from subjecting to severe penalties, fines of up to 20 million dollars or 4 percent of annual revenue whichever is higher [2] and losing trusts from its users. Therefore, researchers should ensure Art. 33 and 35 are in place before deployment in the real-world scenario.

6.1. Conclusion

Blockchain compliance with GDPR for healthcare applications is highly dependent on how the technology is utilized and the architectural design. It seems infeasible to conclude that specific blockchain frameworks or main blockchain characteristics are more compliant than others, it is rather use-case dependent and based on several design aspects that together could build up towards GDPR compliance. This research shows that blockchain may enhance GDPR in some aspects and be challenging with some others. It is important that this topic is being addressed and highlight potential compliance issues to increase adoption and acceptance of the technology in this field. There is no such thing as GDPR-compliant blockchain technology for healthcare, but it might be GDPR-compliant use cases and applications. We encourage future work to address GDPR compliance to get closer to real-world adoption of blockchain technology in the healthcare sector.

REFERENCES

[1] Hal Berghel. Malice domestic: The Cambridge analytica dystopia. Computer, (5):84–89, 2018.

[2] European Commission. Reform of EU data protection rules, 2018. https://gdpr.eu, accessed 2020-06-10.

[3] George J Annas et al. Hipaa regulations-a new era of medical- record privacy? New England Journal of Medicine, 348(15):1486– 1490, 2003.

[4] European blockchain observatory and forum. Blockchain and the gdpr, 2018. https://www.eublockchainforum.eu/reports, accessed 2020-06-13.

[5] Fran Casino, Thomas K Dasaklis, and Constantinos Patsakis. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 36:55–81, 2019.

[6] Tsung-Ting Kuo, Hugo Zavaleta Rojas, and Lucila Ohno-Machado. Comparison of blockchain platforms: a systematic review and healthcare examples. Journal of the American Medical Informatics Association, 26(5):462–478, 2019.

[7] Paolo Tasca and Claudio J Tessone. Taxonomy of blockchain technologies. principles of identification and classification. arXiv preprint arXiv:1708.04872, 2017.

[8] Protection Regulation. Regulation (eu) 2016/679 of the european parliament and of the council. REGULATION (EU), 679:2016, 2016.

[9] Khaled El Emam and Cecilia A´ lvarez. A critical appraisal of the article 29 working party opinion 05/2014 on data anonymization techniques. International Data Privacy Law, 5(1):73–87, 2015.

[10] Henry Kim and Marek Laskowski. A perspective on blockchain smart contracts: Reducing uncertainty and complexity in value exchange. In 2017 26th International Conference on Computer Communication and Networks (ICCCN), pages 1–6. IEEE, 2017.

[11] Primavera De Filippi and Samer Hassan. Blockchain technology as a regulatory technology: From code is law to law is code. arXiv preprint arXiv:1801.02507, 2018.

[12] Paul Kengfai Wan, Lizhen Huang, and Halvor Holtskog. Blockchain-enabled information sharing within a supply chain: A systematic literature review. IEEE Access, 8:49645–49656, 2020.

[13] Alain Giordanengo. Possible usages of smart contracts (blockchain) in healthcare and why no one is using them. 2019.

[14] European Parliamentary Research. Blockchain and the gdpr, 2019. https://www.europarl.europa.eu/RegData/etudes/ STUD/2019/634445/, accessed 2020-06-13. [15]Antonio Jesus Diaz-Honrubia, Alejandro Rodriguez Gonzalez, Juan Mora Zamorano, Jesu´s Rey ime´nez, Gustavo Gonzalez- Granadillo, Rodrigo Diaz, Mariza Konidi, Panos Papachristou, Sokratis Nifakos, Georgia Kougka, et al. An overview of the curex platform. In 2019 IEEE 32nd International Symposium on Computer-Based Medical Systems (CBMS), pages 162–167. IEEE, 2019.

[16] Xiaochen Zheng, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaqun Ordieres-Mere. Blockchainbased personal health data sharing system using cloud storage. In 2018 IEEE 20th International Conference on e- Health Networking, Applications and Services (Healthcom), pages 1–6. IEEE, 2018.

[17] Koosha Mohammad Hossein, Mohammad Esmaeil Esmaeili, Tooska Dargahi, et al. Blockchainbased privacy-preserving healthcare architec- ture. In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), pages 1–4. IEEE, 2019.

[18] M Finck. Blockchain and the general data protection regulation: Can distributed ledgers be squared with european data protection law, 2019.

[19] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD), pages 25–30. IEEE, 2016.

[20] Zhe Xiao, Zengxiang Li, Yong Liu, Ling Feng, Weiwen Zhang, Tha- narit Lertwuthikarn, and Rick Siow Mong Goh. Emrshare: A cross- organizational medical data sharing and management framework using permissioned blockchain. In 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), pages 998–1003. IEEE, 2018. [21]Jens-Andreas Hanssen Rensaa, Danilo Gligoroski, Katina Kralevska, Anton Hasselgren, and Arild Faxvaag. Verifymed–a blockchain platform for transparent trust in virtualized healthcare: Proof-ofconcept. In Proceedings of the 2020 2nd International Electronics Communication Conference, IECC, page 73-80, 2020.

[22] Jens-Andreas Hanssen Rensaa. Transparent healthcare. GitHub, 2020.

[23] Jens-Andreas Hanssen Rensaa. VerifyMed - Application of blockchain technology to improve trust in virtualized healthcare services. Master's thesis, Norwegian University of Science and Technology (NTNU), 2020.

[24] Peng Zhang, Jules White, Douglas C Schmidt, Gunther Lenz, and S Trent Rosenbloom. Fhirchain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal, 16:267–278, 2018.

[25] Anton Hasselgren, Katina Kralevska, Danilo Gligoroski, Sindre A Pedersen, and Arild Faxvaag. Blockchain in healthcare and health sciences—a scoping review. International Journal of Medical Informatics, 134:104040, 2020.

[26] Hawig, David and Zhou, Chao and Fuhrhop, Sebastian and Fialho, Andre S and Ramachandran, Navin. Designing a distributed ledger technology system for interoperable and general data protection regulation--compliant health data exchange: a use case in blood glucose data. Journal of medical Internet research, 21:e13665, 2019

AUTHOR

Anton Hasselgren is a research and PhD in the medical faculty at the Norwegian University of Science and Technology, Trondheim Norway. His main research is is blockchain applications in healthcare.