Tracking Decisions about Granting Access to Health Data: Application Analysis and Requirements

Mohammad Salar Arbabi*, Arlindo F. da Conceição‡, Thiago Garrett*, Jan F. Nygård†§, Roman Vitenberg*
*Department of Informatics, University of Oslo, Norway, emails: {mohamarb, thiagoga, romanvi}@ifi.uio.no
‡Department of Science and Technology, Federal University of São Paulo, Brazil, email: arlindo.conceicao@unifesp.br
†Department of Registry Informatics, Cancer Registry of Norway, Norway, email: jfn@kreftregisteret.no
§UiT The Arctic University of Norway, Norway

2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) | 979-8-3503-3535-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/DAPPS57946.2023.00010

Abstract—**Medical research often requires access to sensitive personal health data. According to GDPR, such access is only possible under certain legal bases, such as consent. Verifiable and secure management of health data access is thus essential for promoting public trust in organizations that manage sensitive health data, for ensuring legal compliance, as well as for motivating patients to participate in research projects and allow access to their health data. In this work, we advocate a blockchain-based approach for verifiable management of sensitive health data access for medical research. We present the life cycle of a medical research project w.r.t. health data access, by identifying the involved entities and their interactions. Important requirements for verifiable management of health data access are also identified. We believe that the advocated approach will contribute to satisfying the identified requirements in the context of the defined life cycle.**

Index Terms—**Blockchain, Smart Contracts, Consent Management, Verifiable Health Data Access, GDPR**

I. Introduction

Medical Research (MR) helps saving millions of lives. Both clinical and epidemiological research requires access to *Health Data (HD)* to improve health and treat diseases [1]. For instance, even simple data such as the incidence of a disease among individuals of different age groups and gender might reveal relevant information. However, HD is highly sensitive, a profitable target for unauthorized access, and its management is subject to numerous regulations, such as *General Data Protection Regulation (GDPR)* [2].

The conflict between the importance of access to HD for MR, and the need to protect individuals' privacy leads to a complex and challenging decision process to grant or deny access to HD. Generally, an MR project needs to be conceived and proposed wherein the proposal needs to specify the aim of the study, the data the project requires access to, and the duration of the access [3]. Moreover, the decision to grant or deny access has to be documented. Regulations such as GDPR specify different justifiable reasons for HD access, i.e. legal bases. One such possible legal base is consent, which provides the right to access HD when the corresponding individual has given informed and explicit consent. As previously given consents may be withdrawn at any time, future access to HD have to be denied to comply with updated consent policies.

All the information related to the factors affecting the decision process needs to be stored in a verifiable manner. The currently deployed healthcare systems suffer from a fundamental flaw: critical decisions about denying or granting access and the verifiability of those decisions rely on significant trust in Data Controllers (DC), e.g healthcare registries. For instance, it is the DCs that provide the log of access to patient HD and the justification for granting the access. There is no way for the patients to verify the integrity of the log or the correctness of the assessment of an MR project proposal, except for blindly trusting the DC. Such a firm reliance on a trusted third party negatively affects patients' incentive to consent to voluntary involvement in MR [4].

To the best of our knowledge, our proposal is the first to take into account the GDPR legal bases for granting HD access, as well as the complete life cycle of the HD access, from project proposal, consent collection/withdrawal, to the end of the project, in a provable verifiable way. According to past studies, individuals would be more willing to trust a consortium of non-colluding entities over a single entity that controls all access to HD [5], which potentially leads to increased participation.

However, we argue that it is not trivial to design such solution, since several trade-offs have to be considered. For instance, there are many steps in processing an HD access request, each step requiring interactions between multiple entities. Such interactions should all be tracked by the management system. At the same time, storing too much information in a publicly readable blockchain may reveal individuals' identities, and may result in storage overhead – a costly resource in blockchain platforms.

In this paper, we advocate a blockchain-based approach for tracking decisions about granting access to health data in its complete life cycle. Our main contributions are:

- The decision process to grant or deny access to HD is distributed to several entities that are all involved in the verifiability of the resulting decisions. In this work, we present the life cycle of a project by identifying entities involved in the decision making process and the interactions between them, and map these entities to the GDPR legal roles.
- We identify verifiability requirements for the interactions between the entities in the life cycle.
- We provide a preliminary discussion of the elements in a blockchain-based approach that can be used to implement the

979-8-3503-3535-4/23/$31.00 ©2023 IEEE
DOI 10.1109/DAPPS57946.2023.00010

life cycle while satisfying the identified verifiability requirements.

The elements consist of a blockchain ledger maintained by a consortium of institutions collecting and curating HD, while every other entity can read the ledger for auditing purposes. Researchers interested in accessing HD are the system's clients, who interact with the DCs through smart contract calls. As a central design element of the proposed approach, we envision using verifiable proofs for decisions related to granting access to HD, which are stored on the blockchain.

II. Background

A. GDPR

The privacy requirements mentioned in EU's *General Data Protection Regulation (GDPR)* [2] demand personal data (such as HD) to be processed lawfully, fairly, and transparently. To comply with GDPR principles, a valid legal base is required for any personal data processing activity. To this end, GDPR defines six legal bases including the consent of data owners. Additionally, GDPR defines limitations about the duration of storage and access to personal data, and requires auditability and verification mechanisms of all the operations on personal data. Furthermore, GDPR mandates multiple roles for organizations accessing personal data. Namely, i) *data controller (DC)*, ii) *data processor (DP)*, iii) *data subject (DS)*, and iv) *supervisory authority (SA)*.

B. Research on Health Data

In healthcare, continuous and significant volume of HD is produced because of the various medical procedures and healthcare services [5]. Healthcare systems include different roles and entities in each country [6], according to regional policies and regulations. However, certain roles and entities involved in the process of providing third parties access to HD can be generalized despite of regional differences. Namely, i) *patients* as DSs, ii) healthcare institutions (HIs) who collect HD from DSs, Iii) health registries storing and maintaining data as DCs, and iv) *research institutions* interested in accessing data as DPs in a healthcare system.

HIs are obliged by law to report every HD that is made to DCs [5]. DCs (such as health registries) are responsible for storing, maintaining, and sharing patients HD. DPs (RIs) require access to HD to perform research and to uncover new patterns that might otherwise remain hidden. In order to get access to HD, DPs need to define, propose, and get approval of a research project and request access to HD.

C. Blockchain and Smart Contracts

Blockchain is an immutable distributed ledger composed of a cryptographically linked sequence of blocks, each containing a total ordered history of transactions issued by clients. The ledger is maintained by nodes in a peer-to-peer network, which operate without any trust assumption regarding each other. A consensus protocol is employed to guarantee the integrity and safety of the ledger, even in the presence of malicious nodes. Blockchains can either be permissionless or permissioned.

Smart contracts (SCs) are automated applications deployed on and protected by blockchain. As a result, SCs possess certain unique features and provide advantages. First, the code implementing the logic behind SCs is immutable and tamper-resistance because it is stored in the blockchain ledger. Second, the execution of SCs is done by consensus nodes without mutual trust in a decentralized manner and finally, SCs enable automation of tasks.

III. Project Life Cycle

GDPR demands that DPs who intend to access HD, provide a list of requirements (such as purpose, duration of access, etc.) for their request. Hence, DPs, DCs, and the SA must agree on a study project definition before access to HD is given to DPs. In this section, we define a GDPR-compliant life cycle for a research project — which we call only **project** for the remainder of this work.

The life cycle of a project consists of four phases [3], namely, i) *Project Proposal* (PP), ii) *Project Approval* (PA), iii) *HD Request*, and iv) *Consent Policy Updates*. A project goes through these phases sequentially and in that order, as shown in Figure 1. We further describe each phase below.

1) Project Proposal: In this phase, in order to propose a project, a DP must first explicitly formulate the study objective. Since MR relies on HD, it is essential to identify whether the required HD does exist, and whether there is enough data so that statistical conclusions can be drawn, i.e. power calculations. Often a DP makes a statistical inquiry to a DC about the required HD. This inquiry is necessary in order for a DC to assess the feasibility of the project, as described below in the second phase. With the statistical results obtained from the inquiry, a DP can then define a study protocol and data management plan, which usually consists of the following details: i) purpose of access, ii) identity of the DC that maintains the HD, ii) data-set they require to access, iii) analytical method they will apply on HD, iv) duration of access to HD to conduct MR, and v) inquired statistical information.

For the remainder of the paper, we will refer to the above mentioned details as *project description (PD)*. At the end of this phase, we say that a project is *proposed*.

2) Project Approval: For a proposed project to get *approved*, it first needs to be considered *feasibly approved* and *ethically approved* by the SA. For the feasibility approval, the SA checks the PD, in particular the power calculation by the DP in the previous phase and the purpose and analytical method DP proposed. As mentioned in Section II-B, certain limitations exist when sharing specific HD that can be utilized for identifying patients. Therefore, if the HD requested by the DP refers to a small set of DSs, the SA may consider the PP to be not feasible [3].

Ethical approval should be performed by the SA. However, in specific cases, DCs rely on their local ethical committee, with certain pre-approved legal and ethical jurisdiction, in

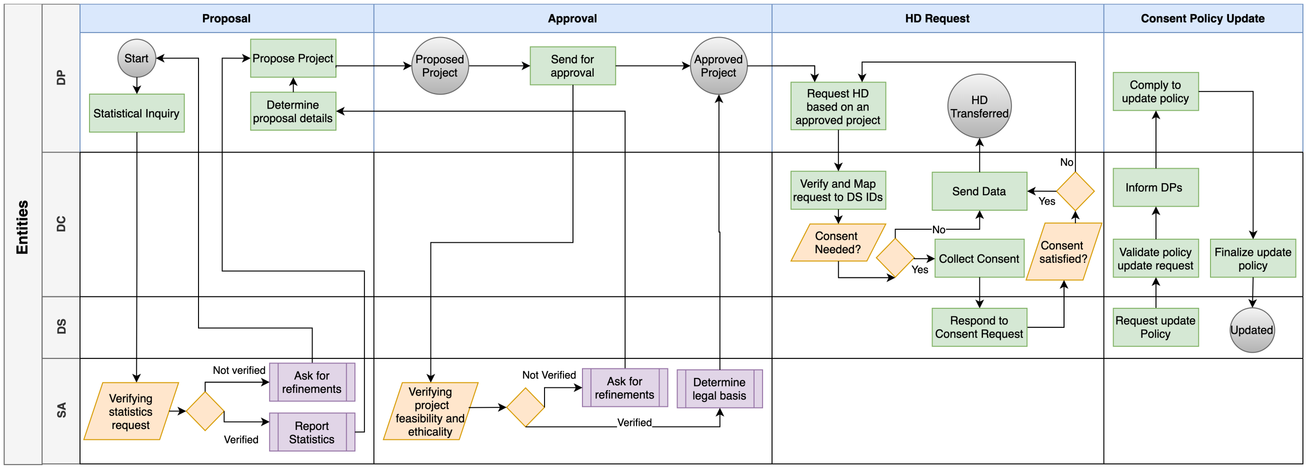

Fig. 1. Project life cycle composed of four phases: Proposal, Project Approval, HD request, and Consent Policy Updates

order to approve a proposed project ethically. If the DC is able to approve the project ethically, they will do so without the need of including the SA [3]. Otherwise, the SA is responsible for approving the project ethically. In the scenario demonstrated in Figure 1 the SA performs the mentioned step. Regardless of which entity (DC or SA) approves ethicality, such entity determines under which legal base the DP will be able to access the HD, as well as the time-frame that the project approval is valid for. These two pieces of information are added to the PD.

Moreover, in case the legal base of the project is determined as consent, the responsible entity for ethically approving the project should also determine the *consent settings (CS)* of the project. The CS determines i) the form of consent DSs should provide (*opt-in* or *opt-out*), ii) time-frame for providing the consent, and iii) time-frame of the project.

In certain scenarios, the SA or the ethical committee of the corresponding DC might ask the DP to conduct refinements on their PP. Refining the proposal could be due to the proposal not satisfying the necessary requirements to be considered feasible or ethical. For instance, DPs cannot ask for certain medical cases that are very rare and distinguishable, which can lead to identifying the patient or proposing scientifically unapproved analytical methods. Furthermore, asking for personal information, such as the national identity number of patients, is an example of why a project might be disapproved ethically. In such cases, the DC or the SA should provide enough reasons for disapproving the PP and allow the DP to refine the proposal. At the end of this phase, we say that a project is *approved*.

3) HD Request: After the project is approved, the DP can execute the project and request HD from the corresponding DC. When DP sends the request to access HD, the DC should verify that the project is approved, within the defined time-frame of validity, and compatible with the DP's request. Moreover, since only the corresponding DC should be aware of the patients' true identity, that DC maps the HD request to the corresponding DSs, but presents only anonymized data (excluding any identifiable information) to DPs. From this phase on, we say that a project is *ongoing*, until the DP has finished using the HD or the time-frame of the project's validity has expired, in which case the project is *finalized*.

4) Consent Policy Update: As per requirements of GDPR, DSs should be able to change the consent policy they have already provided for their data usage. However, DSs can only change their consent policy if they have already participated in a project, and if the consent policy update occurs within the time-frame stated in the consent setting. Otherwise, the DS are updating the consent for a project that already does not have access to their HD anymore (because of the access duration in PA). If the update request is valid, the associate DC will inform DPs about the DS's updated policy. DPs are obliged to comply with the updated consent. They need to inform the DC about the compliance with DSs' policy update so that the policy update phase would be considered final.

IV. Problem Statement

A. System Requirements

We argue that the following five non-functional requirements should be satisfied in each phase of a project: i) lack of reliance on a trusted third party, ii) project description integrity, iii) non-repudiable interactions, iv) verifiability of reasons for denying requests, and v) verifiability of involvement in projects. We further describe each requirement below.

1) Lack of Reliance on a Trusted Third Party: In case the management system for HD access is owned and controlled by a single entity, the controller entity may be vulnerable to security attacks, which can violate DSs' privacy and data integrity. Such security and privacy vulnerabilities, along with a lack of trust in centralized entities can result in less participation of DSs in healthcare research [7]. Therefore, we argue that it is important for a management system to be able to provide access to HD and log to all access without complete reliance on a single trusted entity.

2) Project Description Integrity: It is of crucial importance that the data regarding interactions in different phases of the life cycle remain immutable. No entity should be able to modify information related to PD in the system. If the PD are not tamper-proof, DPs could make modifications after the PA phase, such as changing the legal base for accessing data, or getting access to personal and sensitive HD without DSs' consent or the duration for which they are authorized to process HD which can violate DSs' privacy requirements.

3) Non-Repudiable Interaction: Repudiation threats can be of high concern in healthcare systems [5] if entities are able to deny their actions during the project life cycle. For instance, DSs must not be able to deny giving consent to a specific project. Similarly, DPs must not be able to deny proposing a project, nor requesting HD based on an approved project. Otherwise, if any of the entities can deny the mentioned interactions they have made in different phases of the project, the legality of HD access by DPs could be violated.

4) Verifiability of Reasons for Denying Requests: In certain scenarios and interactions between different entities in the life cycle of a project, requests made by entities could be denied. DSs have the right to withdraw consent to access to their HD and DCs and the SA can deny feasibility or ethicality of a proposed project and ask for refinements.

However, the reason for denying every entities' request should be transparent and verifiable by the entity that made the request. Otherwise, denial of service and not replying to requests could be conducted by entities involved within the system while the entity that made the request is unable to verify their request status.

5) Verifiability of Involvement in Projects: Article 8 of GDPR states that "*Everyone has the right of access to data which has been collected concerning him or her*" [2]. From DSs' point of view, they should have the ability to trace every project they were involved in and to verify and audit their HD as per their provided access policies Additionally, the DCs' ethical committee, or the SA, also needs to audit the compliance of the data processing agreements between DSs, DCs, and DPs.

In current HD access management systems, however, entities do not have a verifiable mechanism for auditing involvements in projects rather than trusting the logs provided to them by the DC [8]. This can violate the GDPR requirements since DSs are not necessarily aware of the projects they are involved in, on a legal basis rather than consent.

B. Research Problem

Current systems that implement the project life cycle rely on the existence of a single trusted entity – in general, DCs are responsible for maintaining the life cycle of the project and handling HD access requests from DPs. Moreover, at present, the process of consent collection from DSs in some healthcare systems, registries, and research institutions still relies on paper-based techniques [9]. There are many ongoing efforts to transform the process of paper-based consent management to electronic-based. Open challenges of this transformation [5] include: i) coarse-grained control over consent permissions and settings, ii) difficulty in handling consent update policies in a timely manner, iii) ethical concerns and errors due to binding consent setting data with intelligent systems, and iv) lack of transparency and DS-centric control.

Our goal is to propose a system for verifiable management of HD to be accessed by DPs, while addressing the threats above. More precisely, the research problem we address in this work is defined below.

Research problem: Design a verifiable management system for HD access that implements the project life cycle, and satisfies the identified system requirements.

V. Blockchain-based approach

In this section, we discuss a blockchain-based approach to propose a verifiable management system to access HD. The solution needs to address the deployment of the project life cycle, as discussed in Section III, while fulfilling the requirements that were mentioned in Section IV-A.

We believe the existence of registries in healthcare systems, which are trusted and supported by law to collect and maintain HD of patients, and the SA, suggests utilizing a consortium blockchain where consortium members should consist of DCs and the SA as demonstrated in Figure 2. However, every entity can read the ledger for auditability purposes. We assume all the interactions conducted in our system are via smart contract calls and digitally signed by the entity that triggers the interaction.

We propose storing the outputs of the interactions on the blockchain ledger as proofs of conducting the interactions for auditability and verifiability purposes. While the main focus of the solution relies on fulfilling the system requirements that were introduced in Section IV, we intend to keep the amount of on-chain stored data to the minimum possible that fulfills the requirements. If additional information is to be stored on-chain, the size of the ledger will grow which makes it a challenge for DCs and the SA to maintain the ledger. However, if sufficient proofs are not stored on-chain, it can violate the project liveness since it would not be verifiable to audit which entity is blocking the progress of the project life cycle. An example is given next.

In the PP phase, DPs need to make a statistical inquiry. The DP can initiate a smart contract (SC) call for the inquiry

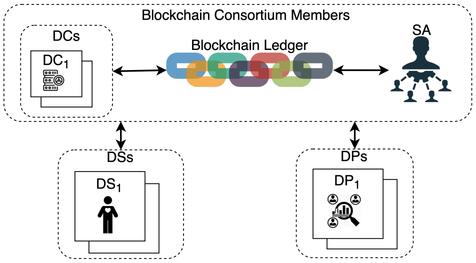

Fig. 2. Illustrating the solution approach

where the output of the SC call will be stored on-chain as a proof of interaction. After receiving the statistical data, the DP proposes a project where a proof of proposal will be stored on-chain for verifiability purposes. Moreover, after assessing the project and storing the proofs of the assessments on the ledger the project will be approved. The requesting DP can ask for HD based on the approved project. The request is implemented via an SC call, and a proof of the request is stored on-chain.

VI. Discussion & Analysis

In this section, we discuss how the proposed approach satisfies the requirements described in Section IV.

A. Fulfilling System Requirements

1) No Reliance on Third Parties: Our proposed approach relies on a consortium blockchain where DCs and the SA are consortium members maintaining the ledger and participating in the consensus protocol. A consortium blockchain can provide limited transparency and view of the ledger, and provide verifiability to specific users known to the system. This can ensure that no single entity is in charge of maintaining access logs to HD and providing it for auditability purposes.

However, mapping requests from DPs to actual DSs' identity could only be done by the associate DC that maintains DSs' HD. Although the only single entity that can conduct this interaction in our system is the associate DC, reliance on the associate DC to conduct this action is due to the privacy requirements of DSs. No other entity should have access to DSs' HD except for the associate DC which is authorized and obliged by law to maintain HD.

2) Project Description Immutability: In our proposed approach, several interactions regarding access to HD are stored on-chain including PD. In our solution, all consortium members (DCs and the SA) have a copy of the ledger and appending any new block to the ledger can only happen after the consortium reaches to a consensus. Hence, PD and proof of conducting interactions between different entities remain immutable in different cycles of a project since each block contains the hash of the previous block, and the ledger is replicated across peers that participate in the network.

3) Non-Repudiable Interactions: Blockchain can ensure non-repudiation of interactions in our proposed management system for HD access since it can provide mutual authentication between involved entities in a project. As a result, different entities cannot repudiate conducting any of the mentioned transactions, in the scope of our proposed system. For instance, a DP can never deny requesting an HD based on an approved project since the proofs of those interactions are signed by themselves and stored on-chain, visible to every consortium member who can verify it.

4) Verifiable Reasons for Denying Requests: In cases where a DP's request for proposing, approving, or requesting HD is rejected, they should be provided with sufficient reasons and information to refine their request. In our approach, we propose to achieve this requirement by storing refinement proofs on-chain to achieve immutability, non-repudiation, and verifiability. To this end, the proof should include a detailed explanation of what aspect of DP's request is not feasible, ethical, or acceptable.

5) Verifiable Involvement in Projects: In order to provide auditability and traceability for DSs, we propose to store verifiable proofs of involvement in projects on the ledger. From DSs' point of view, they need to trace and audit the projects their HD is being used in. To achieve this, an application on DSs' side could be used to read from the ledger and trace every proof of HD transfer they were involved in to provide them with a complete list of the projects. Hence, DSs can audit the project details and verify their involvement in projects either per consent policies they agreed upon or alternative legal bases which satisfies the requirement.

Moreover, since every consortium member has a transparent view of the information stored on-chain, DSs do not need to rely on the access logs that would be provided to them by a single DC. Additionally, the SA can benefit from the same verifiable proofs of involvement of different entities in each project to audit compliance to the agreements between DPs and DCs to enforce GDPR security and privacy requirements.

B. Limitations

1) Multiple DCs Involvement in a Project: In practice, multiple DCs are involved to provide HD of a project. However, DCs should have no knowledge about HD that is being stored by other registries. Several encryption initiatives such as zero knowledge proofs [10] could be utilized to keep the DSs' identity and other information confidential. However, DCs need to establish an authentication mechanism, such as blockchain-based self-sovereign patient identity mechanisms and decentralized identity management schemes in the healthcare sector [11] to be able to map requests of DPs to the same list of DSs' identities without revealing more HD. Challenges of establishing such schemes are still underdeveloped in the existing literature and out of the scope of our study.

2) Project Refinements: In several steps of a project life cycle, the DC or the SA can ask a DP to refine a statistical inquiry, project feasibility, or project ethical assessment. We have proposed a proof of asking for refinements to be stored on-chain. However, the data format and interaction interface for refining each of the requests are not well defined and is usually provided to DPs in plain text [8] in practice. Moreover, the justification and reasoning for denying a request can be subjective to each DC or the SA and differs in each healthcare system and domain. The mentioned issues make it challenging to map the refinement process to concrete smart contract calls and the data to be stored on-chain.

VII. Related Work

Over recent years, many studies have focused on consent collection, storage of consent, and use of collected consent and personal data [12]. Authors of [13] proposed *Consentio*, a consent management platform and designed the world state of the system to provide better scalability of consent collection. Authors have proposed implementation and optimization guidelines and provided results of their experiment w.r.t. scalability design goals. Utilizing permissioned blockchain ledgers has also been studied in [14]–[16] where authors focus on blockchain-based access control protocols for personal data.

Permissionless blockchain has also been proposed in the existing literature for consent management [17], [18]. Since in a permissionless blockchain every user has read access to the blockchain ledger, most of the contributions suggesting a permissionless ledger focus on the confidentiality and privacy requirements of the data being stored on-chain.

Some of the existing literature focus on implementing a consent management system for use cases in healthcare systems that are different from sharing HD for research purposes. Such as consent management for i) clinical trials for a patient-centric access management system to share HD [19], [20], ii) consent mechanisms to access fitness data from fitness service providers [21] or, iii) a domain agnostic consent management system [13], [22] which could be slightly modified to be compatible with various use-cases and requirements.

However, to the best of our knowledge, none of the contributions in the state-of-the-art considered different phases of accessing HD for research purposes. Moreover, consent is one of the six legal bases under which personal data could be accessed by DPs based on GDPR regulations. Within the existing literature, authors are focused on consent collection and storage and accessing HD under other legal bases has remained underdeveloped in the state-of-the-art. Additionally, since the mentioned phases of the project life cycle for accessing HD have not been studied in the existing literature, the associated requirements in each phase (such as verifiability, traceability, auditing, non-repudiation, etc.) have not been addressed in the state-of-the-art which we discuss in Section IV-A.

VIII. Conclusion

In this work we propose a blockchain-based approach for managing HD, providing reduced centralization and improved verifiability. Every step in the life cycle of an MR project is verifiable and non-repudiable. Therefore, by following the proposed approach, a management system for HD access can prevent several different threats from each of the involved entities. In addition, the approach enables fine-grained management of consent according to the GDPR.

In the future, we intend to implement the proposed approach using specific blockchain technologies, in order to evaluate scalability and performance bottlenecks as more DCs, DPs, and DSs join the system. Another research direction consists of designing new privacy schemes to guarantee that DSs' identities will not be revealed even in the presence of colluding DPs that share HD with each other. Finally, we argue that the approach proposed in this work can be extended to support more general scenarios in which GDPR legal bases are required, not limited to healthcare.

Acknowledgment

This research was partially supported by SmartMed Project, Research Council of Norway, project number: 288106.

References

[1] B. Röhrig, J.-B. Du Prel, D. Wachtlin, and M. Blettner, "Types of study in medical research: part 3 of a series on evaluation of scientific publications," *Deutsches Arzteblatt International*, vol. 106, no. 15, pp. 262–8, 2009.

[2] E. Commission, "General data protection regulation (GDPR)." [Online]. Available: https://commission.europa.eu

[3] National Cancer Registry of Norway , Private Communication, 2022.

[4] G. D'Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y.-A. de Montjoye, and A. Bourka, "Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics," *arXiv preprint arXiv:1512.06000*, 2015.

[5] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygård, and R. Vitenberg, "A survey on blockchain for healthcare: Challenges, benefits, and future directions," *IEEE Communications Surveys & Tutorial (IEEECOMST)*, 2022.

[6] L. L. Hagenaars, N. S. Klazinga, M. Mueller, D. J. Morgan, and P. P. Jeurissen, "How and why do countries differ in their governance and financing-related administrative expenditure in health care? an analysis of OECD countries by health care system typology," *The Int. journal of health planning and management*, vol. 33, 2018.

[7] J. Lederman, B. D. Taylor, and M. Garrett, "A private matter: the implications of privacy regulations for intelligent transportation systems," *Transportation Planning and Technology*, vol. 39, 2016.

[8] D. Calvaresi, D. Cesarini, P. Sernani, M. Marinoni, A. F. Dragoni, and A. Sturm, "Exploring the ambient assisted living domain: a systematic review," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, pp. 239–257, 2017.

[9] J. Kaye, E. A. Whitley, D. Lund, M. Morrison, H. J. A. Teare, and K. Melham, "Dynamic consent: a patient interface for 21 century research networks," in *European Journal of Human Genetics*, 2015.

[10] H. Wu, W. Zheng, A. Chiesa, R. A. Popa, and I. Stoica, "{DIZK}: A distributed zero knowledge proof system," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 675–692.

[11] B. Houtan, A. S. Hafid, and D. Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90 478–90 494, 2020.

[12] P. V. Kakarlapudi and Q. H. Mahmoud, "A systematic review of blockchain for consent management," in *Healthcare*, vol. 9, no. 2. Multidisciplinary Digital Publishing Institute, 2021, p. 137.

[13] R. R. Agarwal, D. Kumar, L. Golab, and S. Keshav, "Consentio: Managing consent to data access using permissioned blockchains," in *2020 IEEE ICBC*. IEEE, 2020, pp. 1–9.

[14] D. Di Francesco Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *IFIP international conference on distributed applications and interoperable systems*. Springer, 2017, pp. 206–220.

[15] O. Choudhury, H. Sarker, N. Rudolph, M. Foreman, N. Fay, M. Dhuliawala, I. Sylla, N. Fairoza, and A. K. Das, "Enforcing human subject regulations using blockchain and smart contracts," *Blockchain in healthcare Today*, 2018.

[16] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

[17] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, A. Papanikolaou, and A. Kritsas, "ADvoCATE: a consent management platform for personal data processing in the IoT using blockchain technology," in *International Conference on Security for Information Technology and Communications*. Springer, 2018, pp. 300–313.

[18] V. Jaiman and V. Urovi, "A consent model for blockchain-based health data sharing platforms," *IEEE access*, vol. 8, pp. 143 734–143 745, 2020.

[19] T. Rupasinghe, F. Burstein, and C. Rudolph, "Blockchain based dynamic patient consent: A privacy-preserving data acquisition architecture for clinical data analytics." in *ICIS*, 2019.

[20] G. Albanese, J.-P. Calbimonte, M. Schumacher, and D. Calvaresi, "Dynamic consent management for clinical trials via private blockchain technology," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2020.

[21] M. Alhajri, C. Rudolph, and S. A. Salehi, "A blockchain-based consent mechanism for access to fitness data in the healthcare context," *IEEE Access*, 2022.

[22] M. Davari and E. Bertino, "Access control model extensions to support data privacy protection based on GDPR," in *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 2019, pp. 4017–4024.