Multi-Stakeholder Contract Governance for Medical Data Access Using Distributed Ledgers

1st Mario A. Cypko*
Hahn-Schickard and
IES Lab
University of Freiburg
Freiburg, Germany
mario.cypko@hahn-schickard.de
ORCID: 0000-0003-2944-9357

2nd Charan Annadurai*
ivESK
Offenburg University
Offenburg, Germany
charan.annadurai@hs-offenburg.de

3rd Dominik Welte
ivESK
Offenburg University
Offenburg, Germany
dominik.welte@hs-offenburg.de
ORCID: 0000-0003-0641-6974

4th Aditya Kumar
Hahn-Schickard and
IES Lab
University of Freiburg
Freiburg, Germany
aditya.kumar@hahn-schickard.de

5th Axel Sikora
Hahn-Schickard
Freiburg, Germany
and *ivESK*
Offenburg University
Offenburg, Germany
axel.sikora@hs-offenburg.de
ORCID: 0000-0001-6811-3659

6th Oliver Amft
Hahn-Schickard and
IES Lab
University of Freiburg
Freiburg, Germany
oliver.amft@hahn-schickard.de
ORCID: 0000-0001-6811-3659

***Abstract*—The secure and controlled access to medical data is a critical challenge in modern clinical research. Regulatory frameworks such as the GDPR and the EU AI Act impose strict requirements on data access, privacy, and transparency, making conventional data-sharing processes inefficient and administratively burdensome.**

Our proposed HyperAccess platform aims to digitise and streamline the contractual access management of medical data through Hyperledger Fabric, an enterprise-grade, permissioned blockchain framework. The project introduces a semi-automated access control system that minimizes administrative efforts while maximizing trust among stakeholders, including data holders, data owners, and data users. By employing exclusive channels on Hyperledger Fabric, only stakeholders involved in an agreement are part of the dedicated channel. This paper presents the design principles, technological framework, and potential impact of HyperAccess on multicentre clinical research, offering a scalable, privacy-preserving, and practically validated solution through an initial prototypical implementation.

***Index Terms*—blockchain for healthcare, smart contracts, permissioned blockchain, access control, data governance**

I. Introduction

Despite the growing demand for high-quality medical data in clinical research and AI-driven healthcare applications, accessing these data efficiently remains a challenge. Current processes for obtaining medical data rely on time-consuming and costly paper-based bureaucratic workflows, including manual approvals, ethics committee evaluations, and fragmented legal frameworks [1]–[3]. These manual processes frequently lead to significant delays, restricting timely research and innovation. Furthermore, data silos in hospitals and research institutions create barriers, preventing effective cross-institutional collaboration and limiting researchers' access to diverse, representative datasets necessary for robust AI model training.

A digital, automated and standardised consent management system would be desired, which is also compliant with regulations such as GDPR [4]. GDPR requires that patient data access be explicitly consented to, transparent, and revocable at any time, which many existing systems struggle to accommodate efficiently. Without a verifiable, tamper-proof system for managing permissions, it becomes difficult to track who accessed data, under what conditions, and whether consent was properly managed. Furthermore, traditional access control mechanisms often lack an immutable audit trail, making compliance audits complex and time-consuming. As a result, researchers, institutions, and regulators alike face significant obstacles in balancing data accessibility, privacy, and legal conformity.

The remainder of this paper is structured as follows: In Section II, we outline existing blockchain-based approaches for medical data governance and discuss their limitations. Section III details the methods proposed in our HyperAccess project, which include stakeholder-specific requirements, blockchain architecture, and consent workflows. Section IV presents

The project "HyperAccess" is funded by Baden-Württemberg Stiftung. The authors are grateful for this support.

* Mario A. Cypko and Charan Annadurai are co-first authors.

our results, emphasising the multi-channel design and wallet architecture decisions. Section V discusses the implications, limitations, and further integration opportunities, concluding with insights into future research and potential improvements.

II. State of the art

Several blockchain-based solutions have emerged to address some of the fundamental access management challenges using distributed ledgers as digital notaries. The MedRec project from MIT Media Lab [5] introduced an Ethereum-based system for managing medical records. However, its reliance on a public blockchain leads to high computational costs and scalability issues, making it unsuitable for large-scale clinical research. Similarly, Germany's BloG³ [6] and SouveMed [7] projects focus on identity management and authentication using Hyperledger Aries and Indy but do not provide a comprehensive contract-based data access framework.

Nasrin et al. [8] explore how Self-Sovereign Identity (SSI) and the Zero Trust Model (ZTM) can be combined with Hyperledger Fabric to enhance vaccination data security.

Similarly, Saranya and Murugan [9] examine Electronic Health Records (EHRs) management using Hyperledger Fabric, demonstrating how private data collections (PDCs) can restrict access to patient records while allowing interoperability between healthcare providers.

Wadud et al. [10] extend this concept to remote patient monitoring, integrating IoT sensors and Patient-Centric Agents (PCA) for secure and efficient health data transmission.

Another study by Sheeraz et al. [11] focuses on trustless healthcare data-sharing, proposing an integration of Hyperledger Fabric and InterPlanetary File System (IPFS) to allow traceable data exchange between organisations while maintaining strict access control policies.

While all these studies demonstrate Fabric's effectiveness for secure and permissioned data-sharing, they primarily focus on storing and managing the sensitive medical data directly, whereas we see the requirement to govern data-sharing agreements without handling the data itself, ensuring compliance and trust. As a consequence, data ownership and handling should be in the hands of participating entities. Our proposed HyperAccess-framework offers a fully integrated approach that streamlines multi-institutional access while preserving patient privacy.

III. Methods

A. Background

As motivated above, with the proposed HyperAccess-framework, we aim for a web-based platform enabling efficient data discovery, agreement negotiation, and dynamic consent management among stakeholders, including data owners (patients), data holders (clinics or data repositories), and data users (researchers). To enable multi-institutional access management, HyperAccess introduces a blockchain-based framework leveraging Hyperledger Fabric [12]. Hyperledger Fabric, initially invented by IBM is now part of LF Decentralized Trust, an organisation of the Linux Foundation. Hyperledger Fabric provides a permissioned blockchain infrastructure that can effectively support secure and compliant medical data-sharing scenarios. We investigate the applicability of Hyperledger Fabric to achieve these objectives, focusing on transparency, traceability, and compliance.

B. Objectives

The core methodological approach of HyperAccess focuses on leveraging Hyperledger Fabric's multi-channel architecture to separate contract management from access enforcement, enabling a structured and auditable framework for handling data access requests, approvals, and revocations.

C. Stakeholders' Key Requirements

This section introduces the requirements of the three major stakeholders in an exemplary contract management workflow maintaining full compliance with GDPR and institutional policies. Secondly, it describes the technical architecture, smart contract-based permission management, and the data access workflow.

Based on an internal requirement analysis from multiple German clinical studies, European data holders, and GDPR, the following stakeholder-specific key requirements were identified:

Data Owners (patients or research volunteers) expect explicit, transparent, and dynamically revocable consent management aligned with GDPR. They require interfaces that provide clear overviews and real-time management capabilities for data-sharing requests, modifications, and revocations, alongside comprehensive logging of data access events.

Data Holders (clinics or data repositories) seek secure, reliable mechanisms to digitally create and sign Data Sharing Agreements (DSAs), Tele Service Agreements (TSAs) and Patient Information Consent Forms (ICFs). Their expectations include efficiently managing incoming data access requests, closely monitoring compliance with institutional policies, and securely archiving digitally signed documents for audit purposes.

Data Users (researchers and clinicians) require efficient, standardised workflows to discover relevant health data sets, identify suitable data owners and data holders, establish research networks, and receive automated assistance in the creation of GDPR-compliant agreements and forms. They also need tools to track the status of agreements and ensure compliance.

HyperAccess Administrators focus on maintaining overall system performance, ensuring security standards are met, and assuring regulatory compliance.

D. Core Concepts of Hyperledger Fabric

The HyperAccess system leverages Hyperledger Fabric to specifically address privacy, security, and compliance requirements through its permissioned blockchain structure, distinct channel architecture, smart contract automation, precise endorsement policies, and robust identity management via the Membership Service Provider.

Hyperledger Fabric operates as a **permissioned blockchain**, ensuring that only verified participants can access the network. Each participant belongs to an organisation and has a defined role, creating a secure environment for data sharing.

Channels in Fabric allow isolated communication pathways between specific participants. For example, a hospital and a research organisation could establish a dedicated channel for their interactions, ensuring sensitive information remains inaccessible to other network participants. This enhances privacy and compliance with data protection regulations.

Smart contracts, or chaincode, automate and enforce agreements within the network. These contracts govern workflows such as data access requests, signing DSAs, and granting or revoking permissions. By embedding agreements into the blockchain, Fabric ensures transparency and traceability of actions.

Fabric's **endorsement policies** define which participants must approve a transaction for it to be valid. This allows for precise control over data access, ensuring that actions align with established policies and regulations. For example, specific organisations may be required to approve sensitive transactions, enhancing security and compliance.

The **Membership Service Provider** manages the identities and authentication of the participants, ensuring that only authenticated users can interact with the network, thus adding an additional security layer.

E. Digital Contract and Consent Management Workflow

One of the fundamental concepts of HyperAccess is the utilisation of a web platform, which allows the user to interact with Hyperledger Fabric channels. On this platform, stakeholders initially define their basic policies and preferences regarding data access, see Figure 1. Researchers submit specific requests describing their intended data usage, which triggers the automatic generation of initial contracts. These contracts are subsequently viewed and, if necessary, modified by stakeholders, encompassing a diverse range of roles within the stakeholder group. Roles within the stakeholder group of data holders may include data controllers, data protection authorities, an ethics board, and IT professionals. The insights and modifications made to the contract versions, along with the agreement and digital signature, are meticulously recorded in the designated blockchain channels. In a concrete workflow example, the data requesting process is initiated by researchers conducting metadata-based data searches. Clinical project scientists preliminarily confirm the request, after which automated DSAs, TSVs, and ICFs are generated from templates based on predefined policies and preferences. Ethical board members review and approve these documents. Data owners (patients or volunteers) receive the ICF digitally, confirm their consent electronically, and return the signed form to clinical contract experts. Final copies and data access details are securely shared with researchers, and the entire workflow is transparently logged and auditable via Hyperledger Fabric.

In cases where ethical boards or clinical teams require clarifications or corrections, researchers are promptly informed, allowing iterative refinement of proposals. Data owners retain full control to accept or reject consent requests at any stage, ensuring privacy and GDPR compliance.

IV. Implementation and Results

A. Implementation of User Interfaces

HyperAccess conceptually supports integration with applications developed using Node.js libraries such as `@hyperledger/fabric-gateway` [13], which is currently the most actively developed SDK. This Node.js SDK facilitates blockchain transactions and ledger queries effectively via the Fabric Gateway client API, which abstracts the low-level details of accessing the Blockchain away. Other available SDKs, also leveraging the Fabric Gateway API, include the Go SDK and a Java SDK. Additionally, older client SKDs exist such as a Python versrion or the `fabric-client-flutter` [14] library based on Dart and Flutter exists, but these libraries are deprecated and no longer compatible with newer versions of Hyperledger Fabric, which are using the Gateway client SDK exclusively. The selection of an appropriate SDK should consider factors such as compatibility, maintenance status, and community support.

B. Concept of a Multi-Channel Architecture

HyperAccess is built on Hyperledger Fabric, a permissioned blockchain framework optimised for scalable, privacy-preserving, and regulatory-compliant data access management. The system is designed to ensure that medical data remain securely stored within clinical institutions while providing controlled, auditable, and legally compliant access to researchers. The platform achieves this through smart contract-based permissions that dynamically manage data access requests.

A key architectural feature of HyperAccess is its multi-channel design, which allows for fine-grained control of access permissions and contract management. As illustrated in Figure 2, the architecture consists of at least two distinct channels:

- **Channel 1 - Consent Management Channel:** This channel manages informed consent forms (ICFs), involving all three stakeholders—data owners (patients or volunteers), data holders, and researchers. It ensures

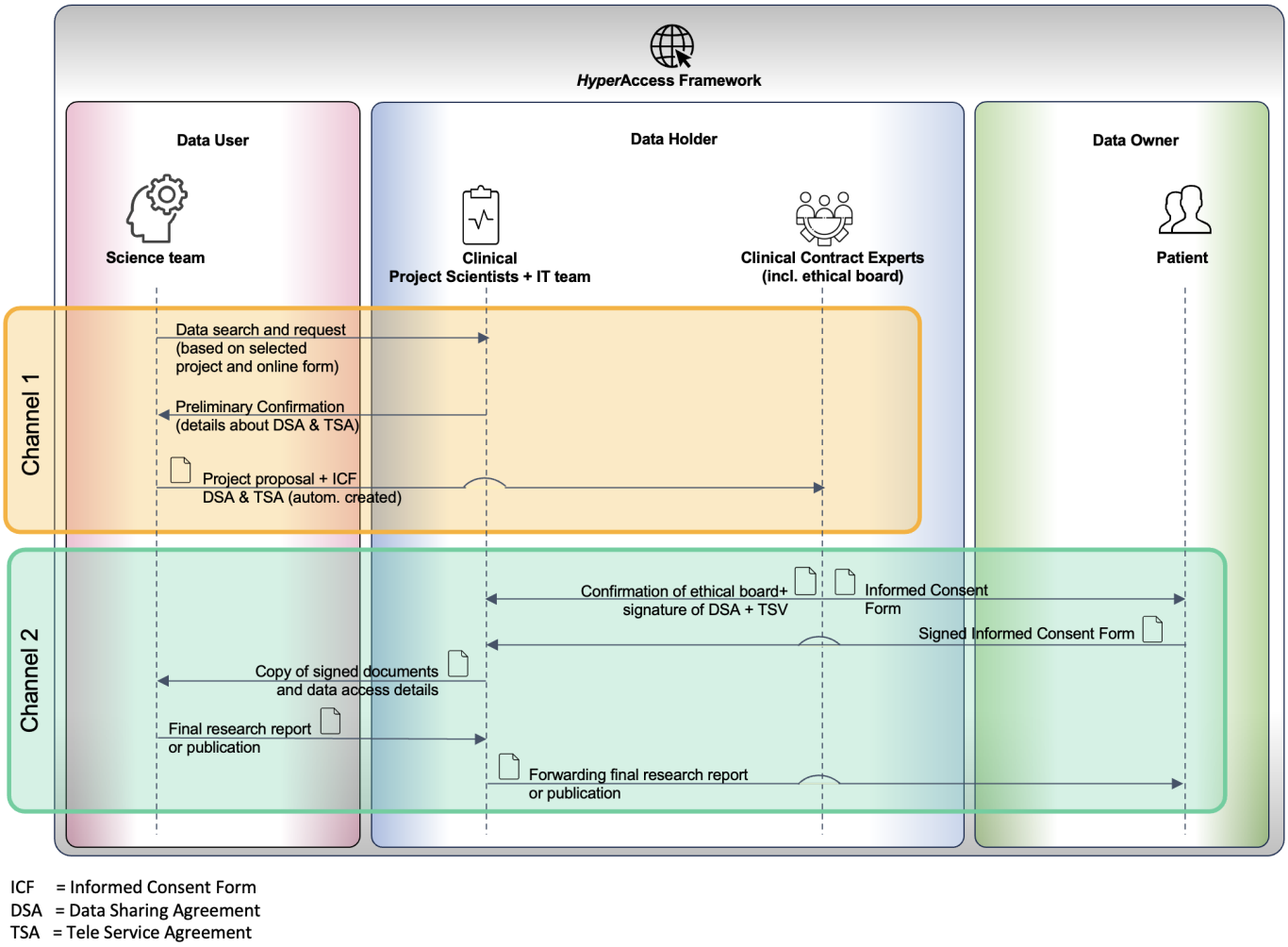

Fig. 1. Example of a contractual workflow to serve a research data request.

that consent changes by data owners are immediately updated, maintaining ongoing compliance with GDPR.

- **Channel 2 - Framework Contract Management Channel:** This channel handles institutional-level agreements (DSA, TSA, and data protection policies). Only the involved institutions have visibility into these contracts, explicitly excluding data owners to maintain the confidentiality of institutional arrangements.

For interactions involving multiple stakeholders (e.g., multicentric studies involving multiple research institutions or clinics), separate dedicated channels are established for each unique institutional interaction. This structured separation of consent management and institutional contract management significantly enhances scalability, data privacy, and regulatory compliance, while maintaining transparency and auditable access logs.

Hyperledger Fabric's test network setup allows only two organisations by default with provisions to add a third. However, this limitation can be scaled, allowing any number of required organisations to participate in a channel. Multiple works suggest that adding multiple organisations can be a resource-intensive process. Increasing the number of organisations in a channel has been shown to introduce non-linear increase in computational overhead, increased CPU usage, and reduced efficiency in cloud environments [15]. Moreover, as more organisations join, network latency and validation delays grow, negatively impacting transaction throughput [16]. Beyond a certain number of participants, synchronization overhead further constrains Fabric's scalability [17]. These limitations require careful network configuration and resource allocation to balance the number of participating organisations with latency and throughput, which is why we grouped all patients of a given institution into a single organisation.

By separating contract management from access enforcement, HyperAccess ensures scalability, privacy, and compliance, while maintaining full transparency of contractual

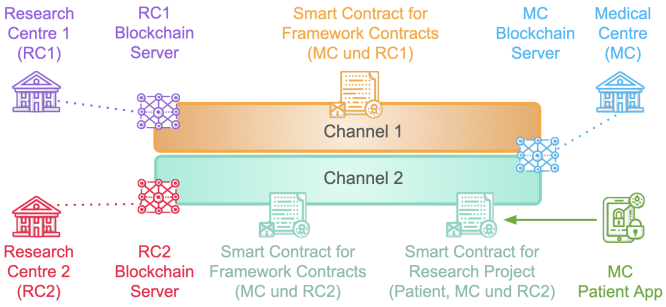

Fig. 2. Concept of two-layered Hyperledger Fabric framework for contractual data management.

obligations and audit trails.

C. Wallet Architecture Analysis

Wallet management is crucial for secure, compliant, and user-friendly blockchain interactions. Our evaluation extensively analysed four wallet management approaches, considering security, usability, complexity, and compliance:

Solution A (Local Wallet Management and Direct Interaction): All wallets are managed by the individual patients and they run their own peer nodes that interact with the blockchain. Though the only solution that is truly decentralised and provides the highest levels of data isolation, it comes with significant drawbacks. Not all patients would have the resources or the technical expertise to run their peer nodes. Even if so, this solution scales poorly.

Solution B (Local Wallet Management and Indirect Interaction): Users independently manage their wallets locally but do not run their own nodes. This solution maximizes security and compliance, as the wallets remain solely with the users, thereby preventing centralised vulnerabilities. However, it places increased responsibility on users to securely manage their wallets. Patients interact with the blockchain through hospital peers, which handle transaction validation and storage. Hospitals serve as trusted intermediaries, distributing the load and enhancing scalability.

Solution C (Custodian Wallet Service and Indirect Interaction): Wallet management is outsourced to either HyperAccess administrators or third-party custodians. While simplifying user and institutional oversight, this approach introduces dependencies on external providers, potentially complicating regulatory compliance. Patients access the system through a simple frontend application, which allows them to perform necessary actions without being exposed to the complexities of the underlying blockchain infrastructure. Wallets can be replaced with passwords and user IDs on the client side. This unfortunately also causes the patients to lose visibility over their transactions and further removes them form the blockchain backend.

Solution D (Indirect Interaction without Wallets): Centralised management of nodes and all transactions are processed through a single wallet. Although it simplifies infrastructure and reduces costs, it introduces severe privacy and trust issues. Similar to Solution C, patients lose visibility and control over their transactions, and the reliance on a single wallet increases the risk of compromise. While this approach may be efficient for smaller networks, it does not align with the security and transparency goals of HyperAccess.

After analysis, Solution B was explicitly identified as optimal due to its strong alignment with GDPR requirements, security best practices, and maximised user autonomy and trust. Despite the slightly increased responsibility placed on end-users, this model ensures maximal compliance and data security, making it the preferred architecture for HyperAccess.

D. Automated Contract Generation and Transparency

HyperAccess significantly reduces administrative workload through the automated generation of contracts (DSAs, TSVs, ICFs) based on predefined templates. These automatically generated documents reduce the manual effort for researchers and data holders, streamlining the data access process. All interactions and contract modifications are transparently logged on the blockchain, providing stakeholders with an immutable and auditable record, ensuring full compliance and accountability at every step.

E. Multi-Stakeholder Verification Mechanism

HyperAccess incorporates a robust multi-stakeholder verification mechanism where a subgroup of pre-verified, trusted data holders, particularly university hospitals, verify new research institutions, patients (including study volunteers and data donors), or other data holders. Universities are particularly suited to this role as stakes due to their established adherence to legal, ethical, and regulatory frameworks. To mitigate conflicts of interest, verifying institutions must be independent of the entity or individuals undergoing verification. Additionally, an appropriate compensation mechanism, consistent with existing hospital practices, is implemented to cover the verification efforts of these trusted stakeholders.

F. Implementation Status and Initial Evidence

At the current stage, a functional backend infrastructure utilizing Hyperledger Fabric has been successfully established. Initial tests have demonstrated the capability to digitally generate contracts, distribute these between stakeholders, and support their acceptance, modification, or rejection in accordance with predefined processes. Preliminary validations indicate the feasibility and effectiveness of automated workflows, contract transparency, and auditability features. However, further practical assessments, specifically involving end-user interactions and interface usability, are necessary to evaluate scalability, system performance under realistic workloads, and practical integration into clinical and research settings.

V. Discussion

The HyperAccess framework addresses several critical challenges inherent in managing health data access, especially concerning GDPR compliance, scalability, and security. By explicitly separating consent management and contract management into distinct channels, HyperAccess effectively reduces complexity, enhances security, and simplifies regulatory compliance. The local wallet management with indirect interaction (Solution B) maximises GDPR compliance and user autonomy, aligning closely with current European regulatory frameworks.

However, some challenges remain. The requirement for users to independently manage local wallets introduces increased responsibility and complexity, particularly for less technically experienced stakeholders. Future work should therefore address improving usability through enhanced user education, intuitive interfaces, or additional support tools to facilitate user adoption and reduce potential errors in key management.

Another limitation includes scalability regarding the maximum number of participants per channel. Although it is possible to add any number of Organisations to a channel, managing numerous separate organisations and channels could potentially become administratively burdensome and resource-intensive.

Future research could explore automated key management tools or user-friendly wallet interfaces to mitigate user responsibility challenges. Additionally, further practical evaluations in real-world scenarios are necessary to assess the long-term sustainability and scalability of the multi-channel approach. An ongoing extension of HyperAccess includes the integration into existing research platforms such as the Bexome[1] patient health tracking app.

The ongoing development foresees the implementation of dedicated dashboards for different stakeholders (patients, clinicians, and researchers), enhancing visibility and usability. The HyperAccess concept is also being integrated with existing patient-facing applications, such as mobile apps, to simplify consent management and enhance user engagement.

VI. Conclusion

HyperAccess introduces a structured, blockchain-based framework designed to enhance privacy, compliance, and efficiency in medical data-sharing workflows. Its multi-channel architecture and local wallet management approach effectively address key requirements for GDPR compliance and secure data access control.

While promising, the approach requires additional usability improvements and further real-world validation to ensure scalability and user acceptance. Continued research and iterative refinements will be essential to fully realise the potential of HyperAccess in streamlining secure medical data sharing between stakeholders.

[1] www.bexome.com — Research app for mobile patient health tracking.

Acknowledgment

The authors would like to thank David Hirsch for the initial requirements analysis and conceptual approaches.

References

[1] R. Houten, M. I. Hussain, A. P. Martin, N. Ainsworth, C. Lameirinhas, A. W. Coombs, S. Toh, C. Rao, and E. St John, "Digital versus paper-based consent from the uk nhs perspective: A micro-costing analysis," *PharmacoEconomics-Open*, pp. 1–13, 2024.

[2] V. N. M. K. Vankayala, "Empowering patients: Digital consent revolution in electronic health records," *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET)*, vol. 15, no. 5, pp. 92–104, 2024.

[3] V. Rahimzadeh, J. Baek, J. Lawson, and E. S. Dove, "A qualitative interview study to determine barriers and facilitators of implementing automated decision support tools for genomic data access," *BMC Medical Ethics*, vol. 25, no. 1, p. 51, 2024.

[4] E. Parliament and C. of the European Union, "Regulation (eu) 2016/679 - general data protection regulation (gdpr)," Online, 2016, accessed: Feb. 26, 2025. [Online]. Available: https://gdpr-info.eu/

[5] MIT, "Medical records on the blockchain (medrec-project)," Online, accessed: Feb. 22, 2025. [Online]. Available: https://github.com/mitmedialab/medrec

[6] B. P. Team, "Blockchain-based health data management for holistic health profiles," Online, accessed: Feb. 26, 2025. [Online]. Available: https://www.blog3.de

[7] SouveMed, "Trustworthy data trustee model for the sovereign management and effective utilization of medical data in sleep research," Online, accessed: Feb. 26, 2025. [Online]. Available: https://souvemed.de

[8] S. Nasrin, "Securing vaccination data using self-sovereign identity, hyperledger fabric and zero trust model," *International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD)*, 2023.

[9] R. Saranya and A. Murugan, "A hyperledger fabric-based system framework for healthcare data management," *7th International Conference on Computing Methodologies and Communication (ICCMC)*, 2023.

[10] M. A. H. Wadud, T. M. A. U. H. Bhuiyan, M. A. Uddin, and M. M. Rahman, "A patient-centric agent assisted private blockchain on hyperledger fabric for managing remote patient monitoring," in *11th International Conference on Electrical and Computer Engineering (ICECE)*. IEEE, 2020.

[11] M. M. Sheeraz, M. U. Abid, M. A. I. Mozumder, M.-i. Joo, M. O. Khan, and H.-C. Kim, "Blockchain system for trustless healthcare data sharing with hyperledger fabric in action," *International Conference on Advanced Communications Technology (ICACT)*, 2023.

[12] L. D. Trust, "Hyperledger fabric," Online, accessed: Feb. 26, 2025. [Online]. Available: https://www.lfdecentralizedtrust.org/projects/fabric

[13] H. Fabric, "Latest release: Sept. 20, 2024," Online, accessed: Feb. 22, 2025. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5/

[14] GitHub, "fabric-client-flutter," Online, accessed: Feb. 22, 2025. [Online]. Available: https://github.com/ghpZ54K8ZRwU62zGVSePPs97yAv9swuAY0mVDR4/fabric-client-flutter

[15] J. Kim, K. Lee, G. Yang, K. Lee, J. Im, and C. Yoo, "Exploring the characteristics of hyperledger fabric in resource consumption," *BRAINS Conference*, 2020.

[16] N. F. B. Idris, M. A. B. Suhaimi, M. S. B. Zakaria, and A. Z. B. Ismail, "Performance analysis of hyperledger fabric on multiple infrastructure setup," *International Conference on Digital Applications, Transformation & Economy (ICDATE)*, 2023.

[17] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, "Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability," *IEEE International Conference on Blockchain (Blockchain)*, 2019.