Health and Technology (2024) 14:451–462
https://doi.org/10.1007/s12553-024-00833-y

ORIGINAL PAPER

Architectural solutions for improving transparency, data quality, and security in eHealth systems by designing and adding blockchain modules, while maintaining interoperability: the eHDSI network case

Sofia Terzi[1,2] · **Ioannis Stamelos**[1]

Received: 30 October 2023 / Accepted: 24 February 2024 / Published online: 2 March 2024

Abstract

Purpose The main purpose and research question of the paper are to investigate the practical application of the eHealth Digital Service Infrastructure (eHDSI) network, with a specific focus on ePrescription (eP), eDispensation (eD), and Patient Summary (PS) use cases, in order to address issues related to transparency, data integrity, privacy, and security in cross-border transactions within this network. The ultimate goal is to determine whether blockchain (BC) technology can effectively resolve these issues without violating General Data Protection Regulation (GDPR) regulations or hindering network interoperability.

Methods The method employed in this study involves conducting empirical research on eHealth networks to propose the incorporation of BC modules in-to network's architecture and services aimed at enhancing and addressing transparency, data integrity, security, GDPR compliance, and maintaining interoperability challenges. Graphical illustrations intended for implementation on private BC networks are offered as a guide for BC architects and DevOps professionals.

Results The paper explains how BC's ledger records transactions and data exchanges transparently. Smart Contracts (SmC) enforce data sharing agreements, ensuring interoperability standards. Access control, encryption, and key pairs enhance security for eHDSI. This integration aims for tamper-proof, auditable transaction history, ensuring data quality. It details GDPR-compliant BC architecture with features like data anonymization, consent management, and mechanisms for data rectification and deletion.

Conclusions The paper concludes by summarizing the key findings of the research. It highlights the role of BC technology in enhancing transparency, security, and interoperability within the eHealth domain while addressing challenges related to data quality and privacy protection. It also acknowledges the need for innovative solutions to align with GDPR requirements. The paper suggests that the insights and recommendations derived from the study can be applied to other industries with similar characteristics, such as high centralization and the exchange of personal data across borders. Overall, the study emphasizes the practical value of BC-supported systems in real-world applications within the eHealth sector.

Keywords Non-repudiation · Provenance · eHealth · ePrescription · Patient summary · Interoperability · Blockchain

1 Introduction

Europe is experiencing significant changes in Information and Communication Technologies (ICT), as outlined in annual or multiannual Action Plans (AP) by the European Union (EU). These plans focus on various key areas such as employment, healthcare, migration challenges, and sustainable finances [1].

One notable AP is the eHealth plan for 2012–2020, emphasizing the potential of ICT in health systems to improve citizens' health, quality of life, and generate financial and

✉ Sofia Terzi
sofiaterzi@csd.auth.gr

[1] School of Informatics, Aristotle University of Thessaloniki, Thessaloniki, Greece

[2] IDIKA SA, 10 Lykourgou str., Athens, Greece

social benefits. E-health involves the extensive use of ICT in healthcare, encompassing its integration into services, development of ICT-driven products, and optimization of processes for holistic healthcare improvements [2].

One significant barrier to eHealth adoption is achieving technical interoperability, acknowledged not only in Electronic Government (eGov) but also in the broader European Interoperability Framework (EIF) [3]. Despite the EIF, the specific needs of eHealth led to the creation of the eHealth EIF (EEIF) by the European Commission (EC) in 2013 and the Refined EEIF (REEIF) was developed in 2015. The eHealth Network (eHN) reached a consensus to adopt REEIF, providing a framework and methodologies to address challenges hindering the exchange of health information, such as diverse standards, data formats, stakeholder complexity, and privacy concerns [4]. The eHN, established under Directive 2011/24/EU, consists of EU Member States (MS) participating voluntarily. MS are obligated to establish National Contact Points for eHealth (NCPeH) to facilitate health-related information exchange within their territories [5].

The establishment of an interoperable eHealth network is a top priority for the EU, crucial for efficient health information exchange, improved healthcare services, and the well-being of citizens. In the evolving eHealth landscape, disruptive technologies like BC gain importance. BC's relevance is emphasized in the EU eGOV Rolling Plan (RP) of 2023, integrated into the IEEE P2141 series standards, focusing on BC for enterprise information systems and combating corruption. Given the historical centralization in the eHealth domain, BC's decentralization capabilities have the potential to enhance transparency, security, and data integrity in health data exchanges. Therefore, this paper seeks to address the following key questions:

RQ1. How can BC technology enhance transparency in the eHealth domain, while ensuring interoperability among the various systems?

RQ2. How can BC enhance security by design in a highly centralized eHealth ecosystem?

RQ3. How can a BC improve data quality in eHealth, networks while safeguarding sensitive data from unauthorized access?

RQ4. How can a BC supported eHealth network be GDPR compliant to protect data sovereignty and rights?

In summary, BC technology holds great promise in transforming the eHealth domain by addressing these critical questions related to transparency, security, data quality, and GDPR compliance. Its decentralized nature offers a unique opportunity to reshape how health data is managed, shared, and protected in a rapidly evolving digital healthcare landscape.

2 Background and research review

The Digital Single Market (DSM) strategy, introduced by the EC in 2015, driven by economic considerations, includes initiatives to remove obstacles in cross-border e-commerce, invest in high-speed broadband infrastructure, and promote innovation in the ICT sector [6]. The DSM has accelerated advancements in various sectors, particularly in cross-border data and services exchange, notably in healthcare. As the exchange of resources becomes crucial, technological advancement, interoperability, and policy alignment are essential for facilitating collaboration among agencies and countries [7].

Facilitating the mobility of EU citizens relies on information exchange infrastructure across MS, particularly in eHealth, allowing Healthcare Professionals (HP) to access medical data of individuals across borders [8]. This exchange faces legal, technical, and security challenges, addressed through decentralized PS and cross-border eP systems. The EU emphasizes healthcare standards enhancement through collaboration, implemented via the Cross-Border Health Directive (2011/24/EU), enabling EU residents to access healthcare services within its boundaries [9]. The expected rise in cross-border medical treatment would increase the exchange of patient information, subject to the EU's GDPR and the Patient's Rights Directive, providing a benchmark for patient confidence in such activities [10].

ICT plays a crucial role in creating essential infrastructure for cross-border data exchange, addressing challenges like interoperability, confidentiality, security, data integrity, and data sovereignty. The Interoperable Europe Act establishes a strategic cooperation mechanism for interoperability. The RP for ICT Standardization, drafted annually by the EC in collaboration with the European Multi-Stakeholder Platform on ICT Standardization, links EU policies with ongoing ICT standardization efforts [11]. The 2023 ICT standardization RP includes BC and Distributed Digital Ledger Technologies policy, recognizing BC's potential to establish a framework for trusted, decentralized services beyond the financial sector [12] by reshaping transactions, information storage, data sharing, and enabling secure sharing of e-health records (EHR) with patient control over data access, addressing communication disruptions, disparities in medical records, and incompatible ICT interfaces among stakeholders [13]. BC applications in healthcare cover secure handling of EHRs, patient consent management, drug traceability, and data security in clinical trials [14].

The eHealth sector is set to improve through strategic measures like the adoption of eP/PS services, enhancing cross-border healthcare access and collaboration among MS [15]. The European Health Data Space (EHDS) regulation, including MyHealth@EU services, builds on the European Patient Smart Open Services (epSOS) pilot and the eHDSI project funded under the Connecting Europe Facility (CEF) and now part of the EU4Health program until 2027 [16]. In this study, the cross-border services offered via eHDSI are commonly denoted as "MyHealth@EU," and the terms eHDSI and MyHealth@EU are utilized interchangeably. The EC launched the EHDS in 2022, with two goals, the first goal is focusing in Primary Use of Data by HP by empowering individuals to have authority over their health data, both within their own nation and when crossing borders, and the second goal is focusing in the Secondary Use of Data, by enhancing the utilization of health data for research, innovation, and policy formulation [17].

Europe is transitioning to a digitally-oriented era, emphasizing a comprehensive approach to secure and transparent eHealth services across MS while facilitating citizen mobility. The paper will delve deeper into the eHDSI network's architecture and core services, particularly eP and PS, identifying research deficiencies and proposing solutions.

Table 1 DG SANTE MyHealth@EU services catalogue from official documentation

Service	Purpose
Communication Services	Facilitate the dissemination of information among multiple stakeholders
Service Desk Services	Address end-users' concerns and issues effectively
Collaboration Services	Enhance the efficiency of stakeholder collaboration and cooperative efforts
Services Requirements	Define a comprehensive set of policy and business requirements derived from regulations, directives, implementing acts, policies, and guidelines, which guide the specification, implementation, and operation
Services Specification	Develop specifications that support the construction of NCPeH and the Service Network
Configuration Services	Facilitate the establishment of the NCPeH Service Network through automated configuration management
Terminology Services	Establish a common clinical data vocabulary (defaulted to English, stored in the MVC) for describing clinical information, with provisions for MS to translate, map, and transcode according to their national policies, resulting in the creation of the MTC
Test And Audit	Define the criteria and audit requirements for entry into the NCPeH Operational Network
Monitoring Services	Collect evidence regarding the performance of core and generic services, requiring mechanisms to gather and report specific performance data for effective performance monitoring
NCPeH Reference Implementation	Simplify the efforts of MSs by providing a jointly developed NCPeH implementation, with the NCPeH technical gateway serving as a pivotal node in the Service Network.

2.1 The eHealth digital services catalogue

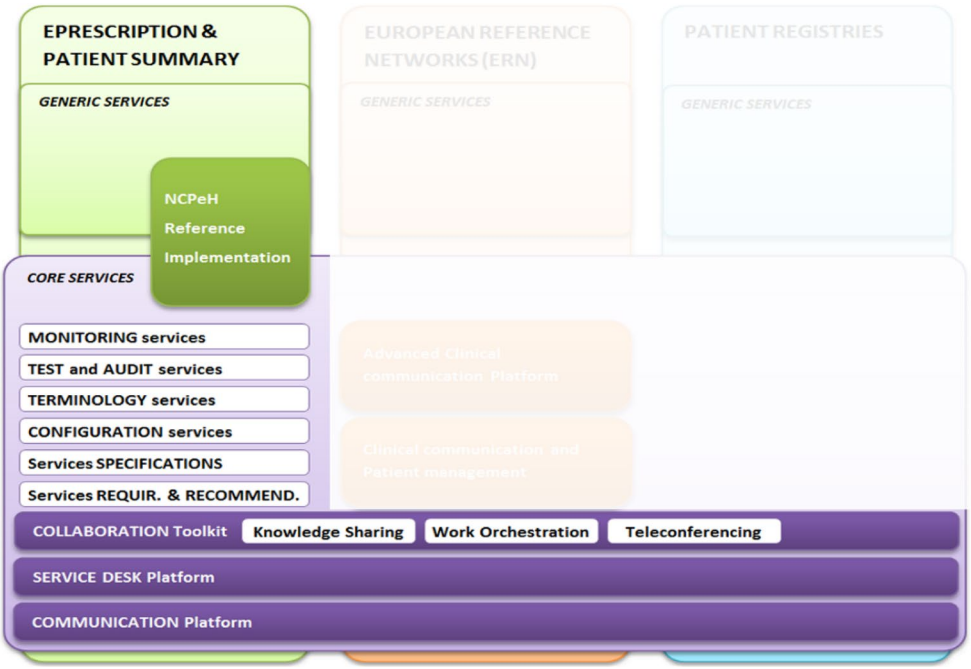
The eHDSI platform facilitates cross-border health data exchange among EU MSs, involving two countries: Country A (patient's home) and Country B (treatment location). Current services include eP and PS, with the upcoming MyHealth@EU network introducing the Original Clinical Document (OrCD) service.

The MS Deploying Country manages the NCPeH, ensuring availability of Generic Services (GS). DG SANTE, as the eHDSI Solution Provider (SP), makes Core Services (CS) accessible for interoperable health data exchange. The eHDSI Service Catalogue (SC) lists CS, and gateway services establish connectivity between national infrastructures and the CS platform. The eP and PS SC, as showcased on the official MyHealth@EU website by reference [18], encompasses a range of offerings depicted in Table 1; Fig. 1. Services like the Monitoring Services, the Terminology Services, encompassing the Master ValueSet Catalog (MVC) and Master Translation/Transcoding Catalog (MTC), must adhere to the eHDSI Requirements Catalog to ensure seamless functionality across MS and to uphold the availability, security, integrity, and interoperability of health data.

2.2 The eHealth digital services requirements catalogue

Under eHDSI, fall two main cross-border use cases, the eP/eD and the PS. The objective of the PS use case [19] is to enable HP in Country B (country of treatment) to access the PS of a patient from Country A (country of affiliation) who is seeking healthcare, whether it be for occasional or regular visits. The patient's rights cross-border Directive (2011/24/EU) describes PS a distinct collection of information that encompasses essential health details necessary for HP to guarantee the delivery of safe and secure healthcare. The normal sequence diagram of the use case is shown in Fig. 2. Currently, MyHealth@EU handles patient authentication based on national policies without using an electronic ID. Each MS is obligated to establish and maintain its national patient and document search database.

The objective of eP/eD use case [20] is to enable a patient to obtain prescribed medication in Country B, when the prescription originates from Country A, where the patient possesses valid healthcare identification. The normal sequence diagram of the use case is shown Fig. 3. Within this sequence diagram, four main functional requirements are identified that need to be addressed. The first, is to ensure



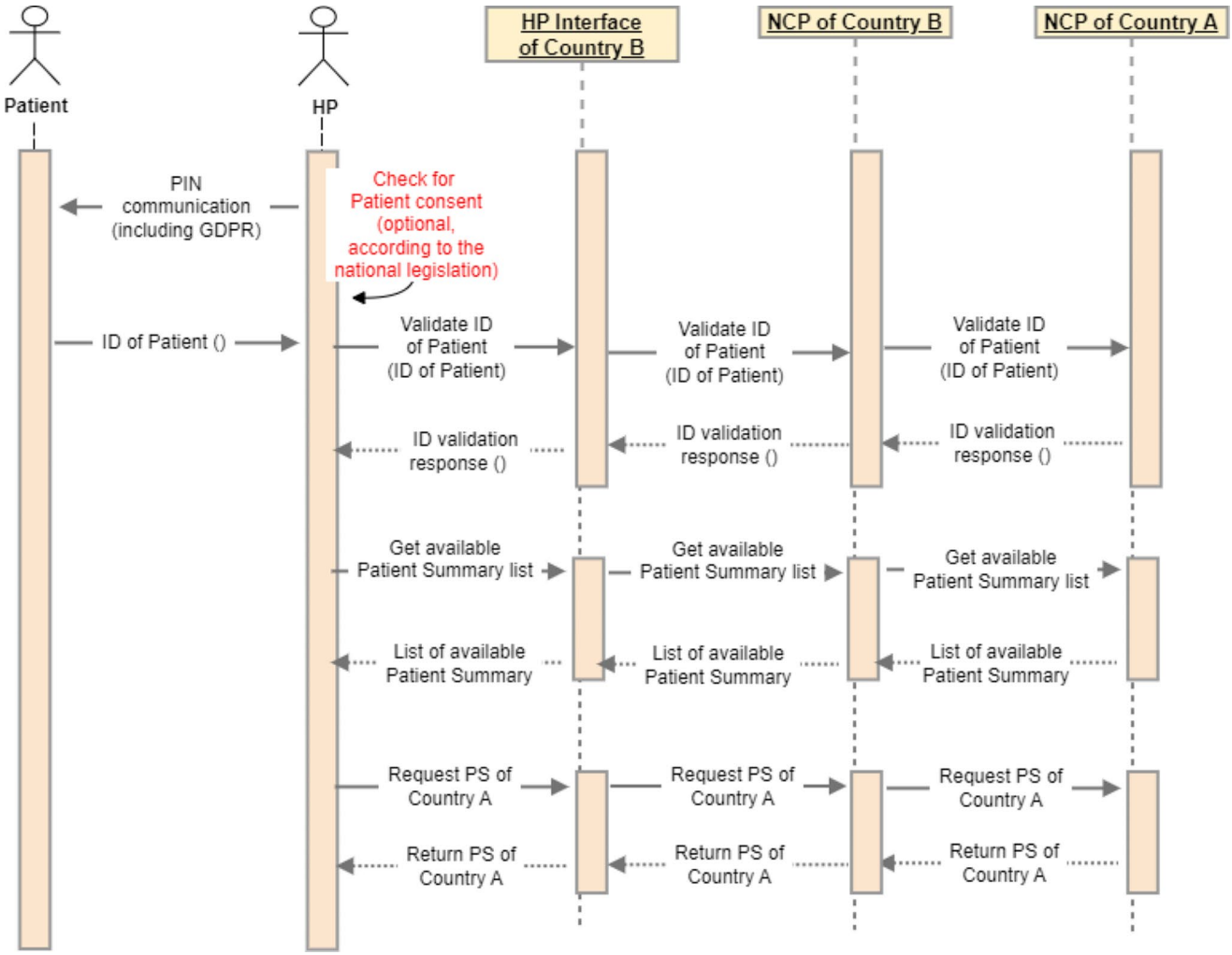


Fig. 1 Service offering > solution provider perspective according to DG SANTE official MyHealth@EU documentation

Fig. 2 Patient summary use case normal sequence according to DG SANTE MyHealth@EU official documentation

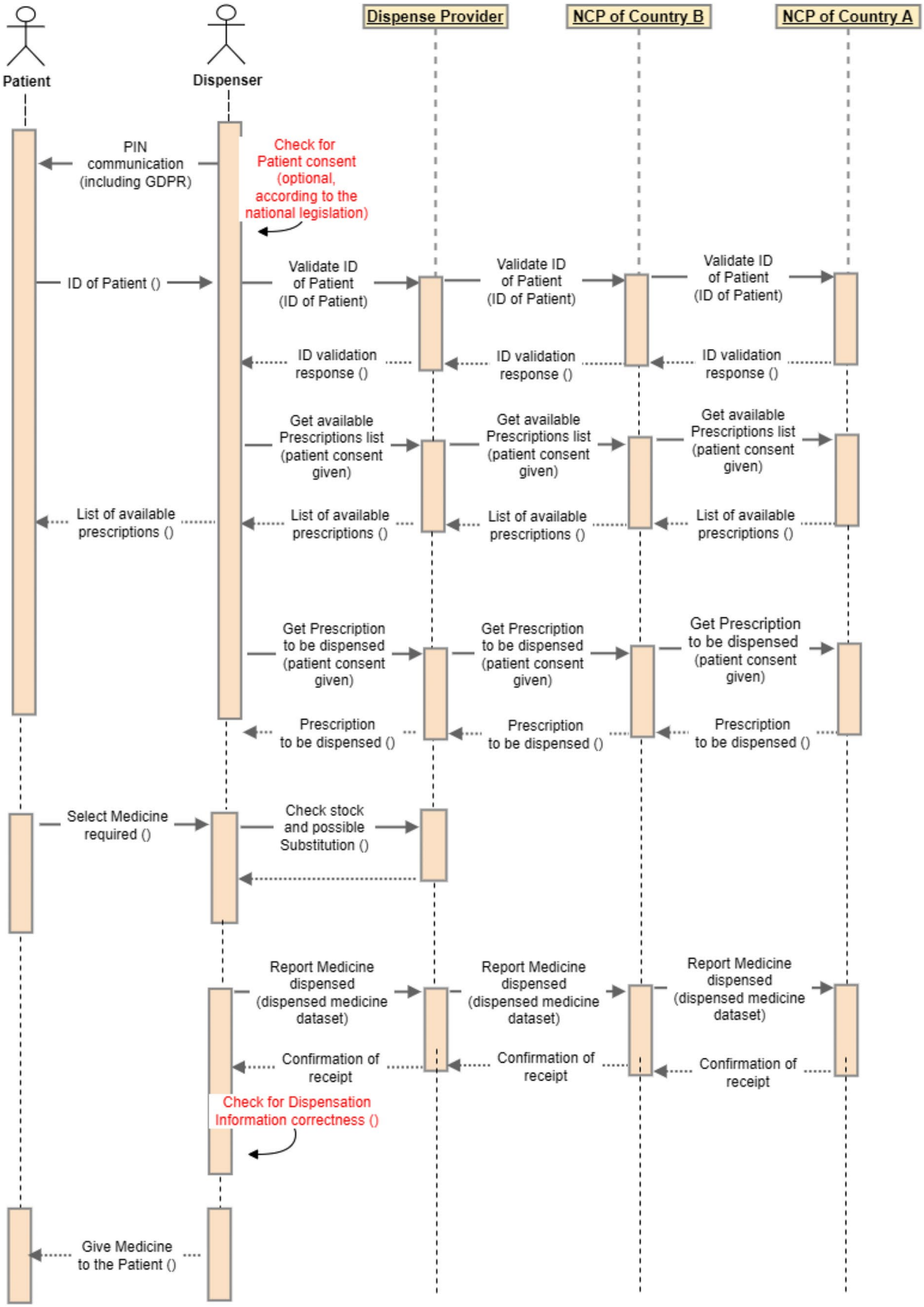


Fig. 3 ePrescription/eDispensation use case normal sequence according to DG SANTE MyHealth@EU official documentation

the security of the service, encompassing aspects like identification, authentication, and patient consent to enable information access between different countries. The second, is to support accurate interpretation of the information, which includes semantic correctness and the correct identification of prescribed medicines. The third, is to define the essential information required to facilitate all stages of the service, including prescription, dispensation, and informing about the dispensation. The fourth, is to provide transparency regarding a country's processes, including its legislation, to other participating countries.

The requirements align with those in the PS use case, focusing on accurately identifying the patient, exchanging high-quality information, and providing the eP document to the HP. The fourth requirement involves managing medication dispensation, following legal regulations in the patient's treatment country. Country B's NCPeH transmits dispensation information to Country A, adhering to MyHealth@EU semantic format.

The new use case, OrCD, empowers Country B's HP to retrieve an OrCD from Country A, associated with a patient seeking medical care. Implementation is supported by an EU Direct Grant in the 2023 EU4Health program. National Competent Authorities are designated for funding, but this paper won't analyze this use case further.

3 Motivation

The foundational document for secure cross-border data exchange in the eHDSI network is the Interoperability Specifications document from DG SANTE [21]. This document establishes NCPeHs as trustworthy entities, requiring mutual recognition of assertions made by NCPeHs. The Circle-of-Trust among participating nations is emphasized, ensuring acknowledgment of assurances from other countries in the eHDSI network. The primary assurances incorporated into the security framework include:

- The accurate identification and authentication of data consumers and producers in Country B.
- The presence of patient consent for participation in the eHDSI.
- Confirmation of a treatment relationship with the patient and authorization of Country B's data consumers and providers by the patient.
- Ensuring the integrity of shared data.
- Verification of the origin and authenticity of the data shared.

The eHDSI MultiLateral Agreement establishes common conduct, assurances, and standards for participants, facilitating the creation of a Circle-of-Trust. This agreement ensures a secure, access-controlled, and resilient environment for confidential health information exchange, with key information requirements:

- The entity or legal authority responsible for issuing and/or authenticating the captured information.
- The identifier of the HP for whom the information was collected, along with their human-readable name.
- The organization or entity under which the HP underwent authentication.
- The time at which the identity information was initiated and when it will expire.
- The specific context in which the HP's identity was verified.
- The legal authentication of all the recorded information by the responsible party, typically the NCPeH-B.

It is crucial to maintain the authenticated identity of healthcare providers persistently within transactions to ensure traceability, linkability, and non-repudiation. Authenticity and data integrity of medical data must be verifiable by recipients, and attached information regarding data source identity must remain unaltered during cross-border transmission.

DG SANTE's Interoperability Specifications document outlines shared requirements for user identification, authorization, transparency, security, data quality, and privacy protection in both PS and eP/eD. Proposing the integration of a BC framework and modules into eHDSI components, communications, and mechanisms, we aim to enhance interoperability and security while aligning with GDPR requirements. The BC network's advantages, such as an immutable ledger, tamper-proof records, decentralized communication, and the use of digital signatures, timestamping, and smart contracts, contribute to achieving these objectives [22, 23].

4 Blockchain in the eHealth digital services infrastructure

To establish the foundation for adopting BC in the eHealth sector, determining the suitable BC network is crucial. Two main types are public and private BCs. Examples of public BCs include Bitcoin and Ethereum, known for digital currency and various business applications [24, 25]. Public networks are open to everyone, but businesses hesitated to expose sensitive information. Private BC networks gained prominence, retaining immutability, decentralization, and automation benefits but with different governance and consensus models. Consensus involves agreement among

nodes on transaction validity, and governance grants authority to permit or forbid network participation [26]. Private BCs often have authorization levels, restricting unauthorized access based on user roles.

Given the crucial considerations of privacy and security in the eHealth sector, a private BC network emerges as the sole viable choice for operations like eP/eD and PS within eHDSI [27]. The network architecture, distinct between national infrastructures and gateways (NCPeH), ensures central connection through NCPeH. Direct communication between foreign NCPeH and national infrastructures is strictly prohibited. Requests must go through the respective MS's NCPeH, functioning as a mediator and gateway for local infrastructure communication.

This high-level network infrastructure, involving multiple NCPeH, can adopt a private BC network for authentication, permissioned authorization, and a consortium model governed by deploying organizations [28]. Each NCPeH functions as a node, preserving ledger data in this decentralized network architecture. The CS, overseen by DG SANTE as the SP, should also participate as BC node in this network, governing new NCPeH entrance. Figure 4 illustrates an architectural design that showcases the incorporation of a private consortium-based BC for specific transactions.

Transactions without personal data are recorded on the BC ledger, crucial for auditing interactions among multiple parties. Each MS maintains existing databases alongside a newly integrated BC component for Trust Services, Data Discovery and Exchange Services, Data Transformation Services, Support Services, and Audit services. The SP retains MVC and MTC services in designated databases, utilizing the BC ledger to store non-sensitive data. The BC acts as a permanent tamper-proof repository, providing evidence of authenticity and non-repudiation while eliminating single points of failure. With only significant auditing-related incidents written on the ledger, the approach minimizes overhead. Detailed implementation for the Audit Trail Service using BC ledgers is explained in Sect. 4.1 for transparency.

4.1 Blockchain for transparency while ensuring interoperability

BC's transparent and immutable ledger provides a comprehensive record of transactions and data exchanges within an ecosystem. SmC automate processes and uphold data sharing agreements, ensuring compatibility with interoperability standards.

The architectural design ensures an indisputable audit trail of transactions on the immutable ledger, devoid of personal information [29]. For the eHDSI network, each NCPeH, must maintain an Audit Trail Writer (ATW) creating an Audit Trail Log (ATL) for transparency. Auditing captures high-level events, while logging deals with lower-level activities, stored in an Audit Repository for retrieval [30]. NCPeH must provide electronic evidence for non-repudiation, ensuring the BC ledger, recording transactions unchangeably, serves as a source of verification, guaranteeing non-repudiation. We propose the system's architecture design along with the necessary BC components for the abovementioned reasons in Fig. 5. The presented procedure

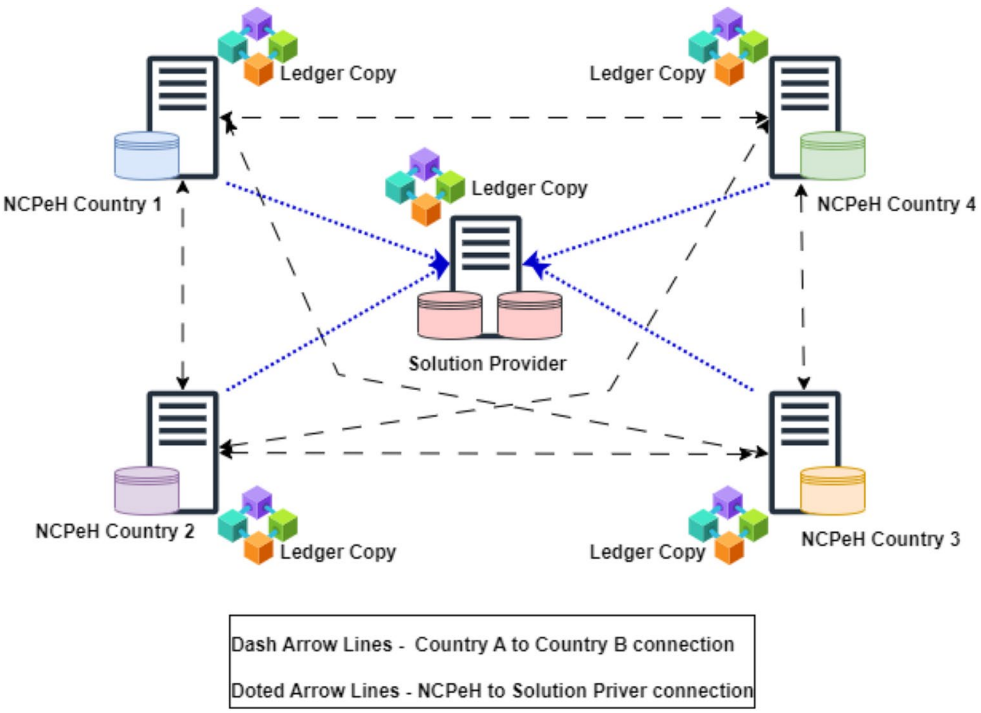


Fig. 4 Blockchain architecture to support eHDSI network

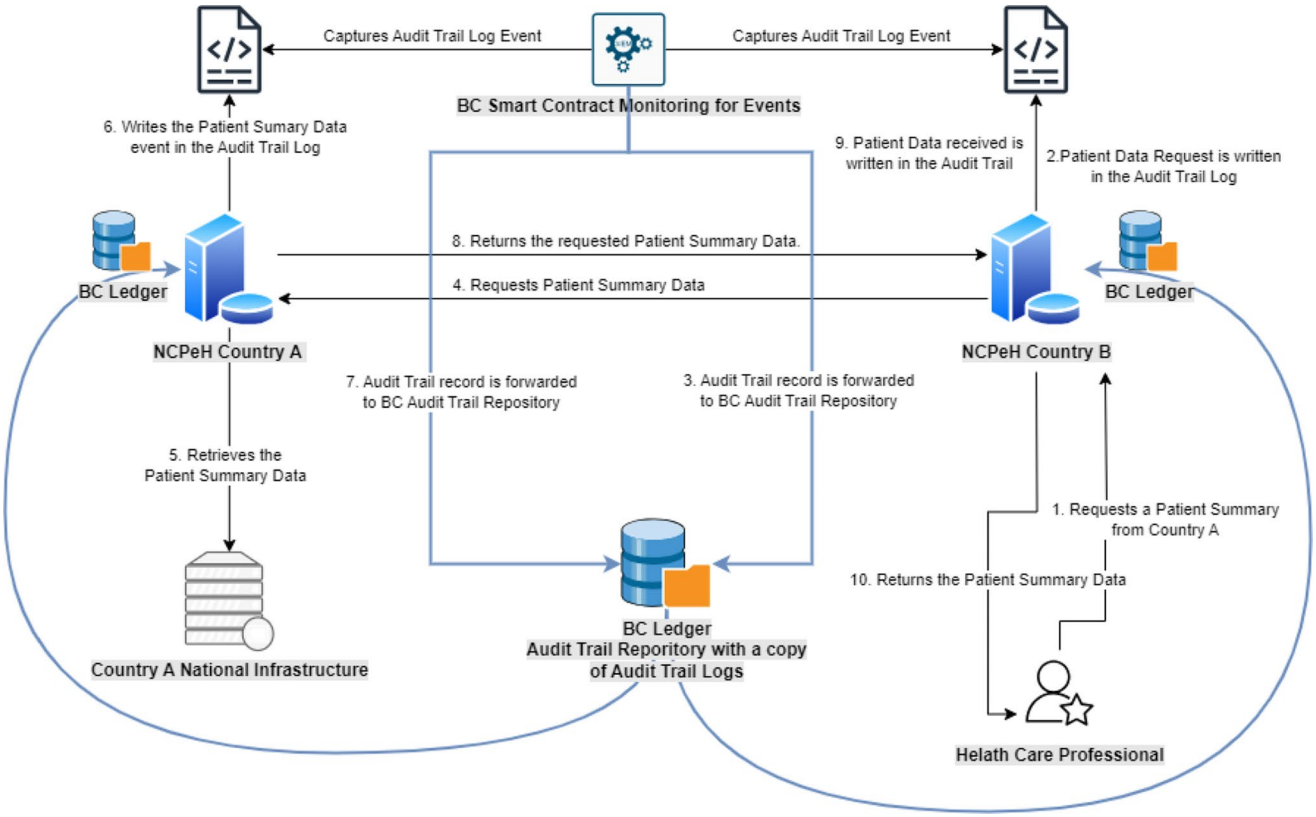


Fig. 5 Blockchain architecture for audit trails logging in patient summary use case

outlines a simplified version of actions during PS retrieval by a HP. Some steps related to processing and additional audit logging are omitted for simplicity.

In this setup, each NCPeH operates as a node in the BC network, holding a copy of the shared BC ledger. A SmC on the BC network monitors the ATL of NCPeH. When a specific event, like a PS request, needs auditing, the SmC is activated after the event is recorded in the ATL, creating a duplicate in the BC's ATL. The BC ATL, stored securely with immutability, includes timestamps and digital signatures for each transaction, following standard BC practices.

The combination of an unchangeable record and the digital signature from the respective NCPeH service ensures transparency, enabling authorized network users or services to view and verify the transaction. The digital signature guarantees non-repudiation of the executing service, and the transaction is permanently recorded on the BC ledger, ensuring data integrity. This design doesn't impact cross-border data exchange or hinder interoperability, as BC records do not alter the evidence structure.

4.2 Blockchain for security in a centralized ecosystem

BC enhances security through cryptographic features and consensus mechanisms, reducing the risk of a single point of failure and enhancing data security [31]. Access control, encryption, and private/public key pairs are integrated into the BC architecture for added security.

In the highly centralized eHealth sector, certain processes, as detailed in Sect. 4.1, can be executed in a decentralized manner. For the ATL in the PS use case, privacy and security can be enhanced by encrypting the audit trail records on the BC ledger. Alternatively, a more secure approach involves storing only the cryptographic digest, a fixed-length string generated by a hash function, ensuring data integrity verification [32] for data integrity verification. The method presumes that the real data is stored in a separate location from the BC. It enables the submission of a data identifier and a corresponding hash of this data to the BC. Subsequently, at any point, it is possible to verify the authenticity of the actual data by comparing it with the hash stored on the BC. Additionally, specific implementations of private BCs, like Hyperledger Fabric (HLF), offer the option to establish distinct channels within the network,

essentially forming subnetworks to restrict access to only specific participants in the network [33].

Consider a simplified private, consortium-based HLF BC network. Each country maintains a ledger copy, even if not interconnected on the eHealth network, allowing for shared data. Connected countries (e.g., Country 1 and 4) exchange sensitive cross-border health data through a private channel, managed by access control lists, ensuring restricted access [34]. Transactions within the private channel remain private, but anchoring records on the main shared ledger provide proof in case of disputes, simplifying evidence provision for dispute resolution while maintaining security and privacy. Countries 1 and 3 are not yet interconnected on the eHealth network, however, they both possess a copy of the main BC ledger.

In terms of security, the consensus mechanism ensures that all network participants or participants in a specific channel must reach an agreement on the validity of a transaction for it to be added to the ledger. If consensus is not achieved, the transaction is marked as invalid, maintaining the security and integrity of the BC network. Additionally, the presence of redundant ledger copies addresses the single point of failure issue, contributing to overall network resilience. Figure 6 illustrates the architectural layout of this BC solution.

4.3 Blockchain for improving data quality and privacy protection

BC ensures data quality by providing a tamper-proof and auditable transaction history. Additionally, BC enables patients to manage their health data consent, ensuring that sensitive information is shared only with authorized entities. Data quality, in this context, refers to the degree to which data conforms to specified requirements, emphasizing measures such as accuracy, completeness, consistency, and validity within a dataset [35]. The BC's ability to establish an auditable chain of interconnected blocks organized in a Merkle tree, in which each leaf value (representing a transaction) can be authenticated by comparing it to the known root, ensures data integrity [36].

The inherent immutability of the BC ledger provides a transparent historical record of all transactions in the network, ensuring verifiability and serving as evidence of data integrity. The consensus process confirms the structural integrity of each transaction, contributing to data consistency and validity. In terms of privacy protection, BC can implement authentication and authorization policies. In a private consortium-based setting, governance rules, such as unanimous decisions for network entry or specific organizations holding decision-making privileges, enhance privacy [37]. In the eHDSI network, the EU SP can be responsible for granting access to organizations meeting prerequisites, creating BC accounts linked to their NCPeH credentials, containing the digital certificate to use for digitally signing transactions [38]. Finally, within a HLF implementation, privacy protection can be further improved by utilizing private channels, as demonstrated in Sect. 4.2.

4.4 Blockchain and GDPR compliance in eHealth sector

A GDPR-compliant BC architecture should include data anonymization, user consent management, and mechanisms for data rectification and deletion. However, as mentioned, consent management, data anonymization, and portability fall beyond the scope of this study.

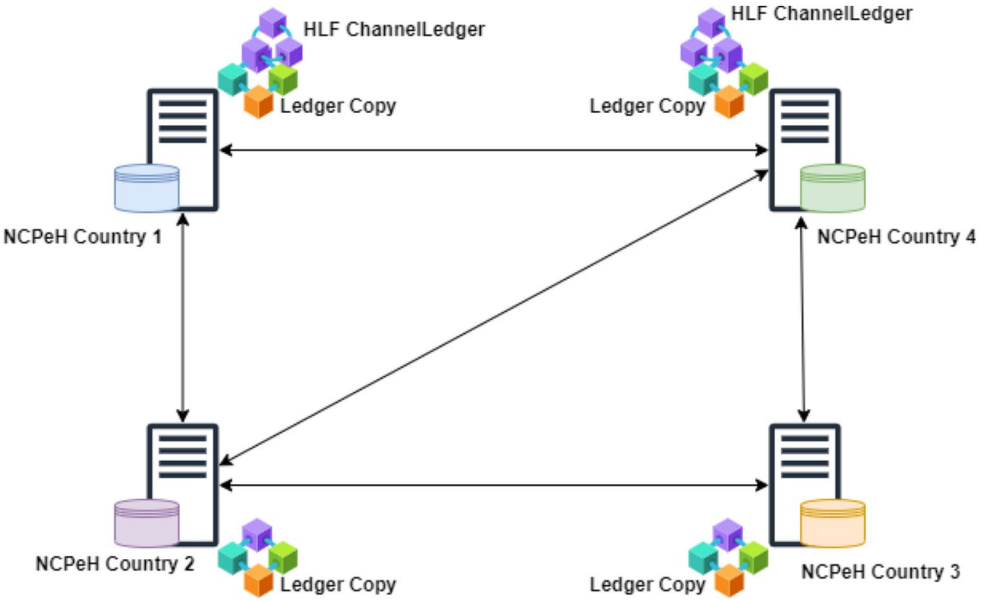


Fig. 6 Hyperledger Fabric Blockchain with private channel

The GDPR poses challenges for businesses adopting BC technology, especially in relation to data protection, privacy, consent management, and data deletion/modification [39]. BC's append-only ledger, once validated, prevents erasure or alteration, a challenge when individuals seek data control or updates due to inaccuracies.

To address GDPR compliance challenges with BC adoption, two approaches can be implemented. Firstly, personal data can be excluded from the ledger, and if necessary, stored in a separate off-chain database, using anchoring techniques for data integrity. A linkage for the hash that is stored on-chain can then be removed from the off-chain data, and this leads to a logical deletion of the data. Secondly, a consensus mechanism designed for block removal from the BC could be established, ensuring informed consent from each node or governing authority [40].

An alternative approach to ensure GDPR compliance involves storing data in an encrypted format on the ledger. However, this method is not recommended for personal or sensitive data due to the uncertainty surrounding the future security of encryption algorithms and the potential vulnerability of the data to decryption, as observed with previous encryption methods.

5 Discussion

Our research has limitations, focusing on network and service aspects of eHDSI's cross-border health data exchange, excluding examination of processes between NCPeH and local infrastructures. This limitation does not compromise research quality within this network segment. Future studies should explore issues related to informed consent management, anonymization, and data portability. The adoption of BC in the eHDSI network may introduce additional overhead with increased cross-border transactions. Private BCs proposed in solutions may cause minor delays and impose additional costs on MS. Anticipation of new services under MyHealth@EU by 2027, including OrCD, laboratory results, and images, along with EHDS regulation, will pose challenges to eHealth network design and delivery as it, will necessitate even greater conformity with eHealth standards aimed at safeguarding and fortifying the security of sensitive eHealth data.

6 Conclusions

In conclusion, our study explores how BC enhances transparency in eHealth, offering an auditable record and automation through SmCs. The architectural design ensures secure data storage, non-repudiation, and maintains interoperability without impeding data exchange. BC enhances security in eHealth by leveraging cryptographic features, consensus mechanisms, and decentralized distribution. It contributes to data quality by providing a tamper-proof transaction history. In privacy protection, BC can enforce access policies in a consortium setting. GDPR compliance challenges involve reconciling BC's immutability with rights like the right to be forgotten, suggesting solutions such as off-chain storage and consensus mechanisms. Our findings are applicable beyond eHealth to sectors with centralized structures, personal data, and cross-border data exchange needs, emphasizing BC's practical value in real-world scenarios.

Acknowledgements One of the authors is employed by an organization fulfilling the role of a National Contact Point for eHealth, and no additional acknowledgments are deemed necessary.

Author contributions The contributions of the two authors remain unchanged, with no additional input.

Funding This research has not received any funding.

Code Availability Not applicable.

Declarations

Ethical approval Not applicable.

Consent to participate Not applicable.

Consent for publication Both authors have provided their consent for publication.

Conflicts of interest One of the authors is affiliated with an organization that serves as the National Contact Point for eHealth, and no further conflicts or competing interests have been identified.

References

1. International Partnerships European Union. (2023). Action plans. https://international-partnerships.ec.europa.eu/action-plans_en.
2. European Commission. (2012). eHealth Action Plan 2012–2020 - Innovative healthcare for the 21st century. https://health.ec.europa.eu/system/files/2016-11/com_2012_736_en_0.pdf.
3. Currie WL, Seddon JJM. A cross-national analysis of eHealth in the European Union: some policy and research directions. Inf Manag. 2014;51(6):783–97. https://doi.org/10.1016/j.im.2014.04.004.
4. d'Hollosy WON, van Velsen L, Henket A, Hermens H. (2018). An Interoperable eHealth Reference Architecture for Primary Care. In 2018 IEEE Symposium on Computers and Communications (ISCC) (pp. 01090–01095). Natal, Brazil. https://doi.org/10.1109/ISCC.2018.8538576.
5. Quinn P, De Hert P. The patients' rights Directive (2011/24/EU)–Providing (some) rights to EU residents seeking healthcare in other Member States. Comput Law Secur Rev. 2011;27(5):497–502. https://doi.org/10.1016/j.clsr.2011.07.010.

6. Lutz SU. The European digital single market strategy: local indicators of spatial association 2011–2016. Telecomm Policy. 2019;43(5):393–410. https://doi.org/10.1016/j.telpol.2018.10.003.
7. Palma FNS. (2022). Interoperability Challenges and Critical Success Factors in the Deployment of Cross-border Digital Medical Prescriptions in Finland and Estonia. In 2022 IEEE International Conference on Digital Health (ICDH) (pp. 60–65). https://doi.org/10.1109/ICDH55609.2022.00018.
8. Martino R, D'Antonio S, Coppolino L, Romano L. (2017). Security in Cross-Border Medical Data Interchange: A Technical Analysis and a Discussion of Possible Improvements. In 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC) (pp. 317–322). https://doi.org/10.1109/COMPSAC.2017.209.
9. Kierkegaard P. E-Prescription across Europe. Health Technol. 2013;3:205–19. https://doi.org/10.1007/s12553-012-0037-0.
10. Baeten R, Palm W. Preserving general interest in healthcare through secondary and soft EU law: the case of the patients' rights directive. Social Services of General Interest in the EU; 2013. pp. 385–412.
11. Galletta A, Ardo O, Celesti A, Kissa P, Villari M. (2017). A Recommendation-Based Approach for Cloud Service Brokerage: A Case Study in Public Administration. In 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC) (pp. 227–234). https://doi.org/10.1109/CIC.2017.00038.
12. EuropeanCommission.(2023).RollingPlanonICTStandardization - Blockchain and Distributed Digital Ledger Technologies. https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/blockchain-and-distributed-digital-ledger-technologies-rp2023.
13. Mettler M. (2016). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1–3). https://doi.org/10.1109/HealthCom.2016.7749510.
14. Junaid, S. B., Imam, A. A., Balogun, A. O., De Silva, L. C., Surakat, Y. A., Kumar,G., … Sahalu, Y. (2022). Recent Advancements in Emerging Technologies for Healthcare Management Systems: A Survey. Healthcare, 10, 1940. https://doi.org/10.3390/healthcare10101940.
15. Katehakis DG, Pangalos G, Prentza A. A European ehealth space for moving cross-border eprescription and patient summary services forward. Transforming Government: People Process Policy. 2016;10(3):478–504.
16. Bruthans J, Jiráková K. The current state and Usage of European Electronic Cross-border Health Services (eHDSI). J Med Syst. 2023;47:21. https://doi.org/10.1007/s10916-023-01920-9.
17. European Commission. (2022). European Health Union: A European Health Data Space for people and science. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2711.
18. European Commission. (2018). Services Provision Blueprint, eHealth DSI –ePrescription and Patient Summary. https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/MyHealth@EU+Service+Offering?preview=/888398047/888398048/eHDSI_ServiceCatalogue-ServiceDelivery-OveralDeployment-Plan_V2.8_20180621.pdf.
19. DG SANTE, CEF eHealth DSI. (2023). Patient Summary Functional Specifications. https://webgate.ec.europa.eu/fpfis/wikis/download/attachments/888805070/PS%20functional%20requirements_v2.22.pdf?version=1&modificationDate=1629903878526&api=v2
20. DG SANTE, CEF eHealth DSI. (2023). ePrescription Functional Requirements. https://webgate.ec.europa.eu/fpfis/wikis/download/attachments/888805081/eP%20functional%20requirements_v2.23.pdf?version=1&modificationDate=1629903879393&api=v2
21. DG SANTE, CEF eHealth DSI. (2023). Interoperability Specifications. https://eceuropaeu.sharepoint.com/:b:/r/teams/GRP-eHDSIMSCommunitiesand-WorkGroups/Shared%20Documents/General/eHDSI%20INTEROPERABILITY%20SPECIFICATIONS/W7/Final%20Updates%207.0.0/eHDSI_Interoperability_Specifications_v7.00.pdf?csf=1&web=1&e=6qPIud.
22. Viriyasitavat W, Hoonsopon D. Blockchain characteristics and consensus in modern business processes. J Industrial Inform Integr. 2019;13:32–9. https://doi.org/10.1016/j.jii.2018.07.004.
23. Karthiga M, Dhivya P, Sankarananth S, Santhi V. (2023). Chapter 9 - Blockchain-based incessant, user-friendly, secure, and unlimited patient care services and manage-ment. In M. M. Ghonge, P. N., A. Das, Y. Wu, & O. Pditors, Unleashing the Poten-tials of Blockchain Technology for Healthcare Industries (pp. 153–173). Academic Press. ISBN 9780323994811. https://doi.org/10.1016/B978-0-323-99481-1.00002-X.
24. Lischke M, Fabian B. Analyzing the Bitcoin Network: the First Four years. Future Internet. 2016;8(1):7. https://doi.org/10.3390/fi8010007.
25. Vujičić D, Jagodić D, Ranđić S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. In 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1–6). https://doi.org/10.1109/INFOTEH.2018.8345547.
26. Zheng Z, Xie S, Dai H, Chen X, Wang H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557–564). https://doi.org/10.1109/BigDataCongress.2017.85.
27. Tandon A, Dhir A, Islam AKMN, Mäntymäki M. Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda. Comput Ind. 2020;122:103290. https://doi.org/10.1016/j.compind.2020.103290.
28. Zhang A, Lin X. via Consortium Blockchain J Med Syst. 2018;42:140. https://doi.org/10.1007/s10916-018-0995-5. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems.
29. Al-Khateeb H, Epiphaniou G, Daly H. Blockchain for Modern Digital Forensics: the chain-of-Custody as a distributed Ledger. In: Jahankhani H, Kendzierskyj S, Jamal A, Epiphaniou G, Al-Khateeb H, editors. Blockchain and Clinical Trial. Advanced Sciences and Technologies for Security Applications. Springer; 2019. https://doi.org/10.1007/978-3-030-11289-9_7.
30. DG SANTE, CEF eHealth DSI. (2023). NCPeH Architecture Specifications. https://eceuropaeu.sharepoint.com/:w:/r/teams/GRP-eHDSIMSCommunitiesand-WorkGroups/_layouts/15/Doc.aspx?sourcedoc=%7B1C2AF67B-2580-44C4-8B3B-101F81C0BE9D%7D&file=eHDSI_NCPeH_Architecture_Specifications_v7.0.0.docx&action=default&mobileredirect=true
31. Gope P, Thwin TT, Vasupongayya S. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. Journal of Healthcare Engineering, 2019, 8315614. https://doi.org/10.1155/2019/8315614.
32. Kalis R, Belloum A. (2018). Validating Data Integrity with Blockchain. In 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 272–277). https://doi.org/10.1109/CloudCom2018.2018.00060.
33. Li D, Wong WE, Guo J. (2019). A Survey on Blockchain for Enterprise Using Hyperledger Fabric and Composer. In 2019 6th International Conference on Dependable Systems and Their Applications (DSA) (pp. 71–80). https://doi.org/10.1109/DSA.2019.00017.
34. Konashevych O, Poblet M. (2019). Blockchain Anchoring of Public Registries: Options and Challenges. In Proceedings of the 12th International Conference on Theory and Practice of

Electronic Governance (ICEGOV '19) (pp. 317–323). ACM. https://doi.org/10.1145/3326365.3326406.
35. Liu C, Nitschke P, Williams SP, et al. Data quality and the internet of things. Computing. 2020;102:573–99. https://doi.org/10.1007/s00607-019-00746-z.
36. Hasselgren A, Kralevska K, Gligoroski D, Pedersen AS, Faxvaag A. Blockchain in healthcare and health sciences—A scoping review. Int J Med Informatics. 2020;134:104040. https://doi.org/10.1016/j.ijmedinf.2019.104040.
37. Murthy CVNUB, Shri ML, Kadry S, Lim S. (2020). Blockchain-Based Cloud Computing: Architecture and Research Challenges. *IEEE Access, 8*, 205190–205205. https://doi.org/10.1109/ACCESS.2020.3036812.
38. Khan S, et al. A Survey on X.509 Public-Key infrastructure, Certificate revocation, and their modern implementation on Blockchain and Ledger technologies. IEEE Commun Surv Tutorials. 2023. https://doi.org/10.1109/COMST.2023.3323640.
39. Truong NB, Sun K, Lee GM, Guo Y. IEEE Trans Inf Forensics Secur. 2020;15:1746–61. https://doi.org/10.1109/TIFS.2019.2948287. GDPR-Compliant Personal Data Management: A Blockchain-Based Solution.
40. Haque AB, Islam AKMN, Hyrynsalmi S, Naqvi B, Smolander K. GDPR compliant Blockchains–A systematic literature review. IEEE Access. 2021;9:50593–606. https://doi.org/10.1109/ACCESS.2021.3069877.