

Article

Addressing the Interoperability of Electronic Health Records: The Technical and Semantic Interoperability, Preserving Privacy and Security Framework

Adetunji Ademola *, Carlisle George * and Glenford Mapp

Department of Computer Science, Middlesex University, The Burroughs, London NW4 4BT, UK;
g.mapp@mdx.ac.uk

* Correspondence: aa4802@live.mdx.ac.uk (A.A.); c.george@mdx.ac.uk (C.G.)

Abstract: Interoperability has become crucial in the world of electronic health records, allowing for seamless data exchange and integration across diverse settings. It facilitates the integration of disparate systems, ensures that patient records are accessible, and enhances the care-delivery process. The current interoperability landscape of electronic health records is saddled with challenges hindering efficient interoperability. Existing interoperability frameworks have not adequately addressed many of the challenges relating to data exchange, security and privacy. To address these challenges, the TASIPPS (Technical and Semantic Interoperability, Preserving Privacy and Security) framework is proposed as a comprehensive approach to achieving efficient interoperability. The TASIPPS framework integrates robust security and privacy measures, providing real-time access to electronic health records that enable precise diagnoses, timely treatment plans and improved patient outcomes. The TASIPPS framework offers a holistic and effective solution to healthcare interoperability challenges. A comparison of the framework with existing frameworks showed that the TASIPPS framework addresses key limitations in privacy, security, and scalability, while providing enhanced interoperability across distinct healthcare systems, positioning it as a more comprehensive solution for modern healthcare needs.

Keywords: interoperability; electronic health records; semantic; security; privacy; healthcare outcomes; framework



Citation: Ademola, A.; George, C.; Mapp, G. Addressing the Interoperability of Electronic Health Records: The Technical and Semantic Interoperability, Preserving Privacy and Security Framework. *Appl. Syst. Innov.* **2024**, *7*, 116. <https://doi.org/10.3390/asi7060116>

Academic Editor: Christos Douligeris

Received: 2 August 2024
Revised: 11 November 2024
Accepted: 13 November 2024
Published: 19 November 2024



Copyright: © 2024 by the authors. Published by MDPI on behalf of the International Institute of Knowledge Innovation and Invention. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

1.1. Overview

Interoperability refers to two or more systems or applications sharing and utilizing information or data [1–3]. In healthcare, interoperability encompasses the seamless and secure exchange of electronic health information across different systems and settings, enabling healthcare providers to access and share patient data efficiently. Interoperability not only improves care coordination and patient outcomes but also facilitates more informed decision-making, advancing the overall quality of healthcare services [4]. Despite the numerous benefits, there are significant challenges regarding the interoperability of electronic health records, related to data exchange, security, and privacy.

The World Health Organization (WHO) has supported digital health for over two decades, helping to establish the science-based discipline of digital health [5]. This long-term commitment underscores the importance of creating robust frameworks that address challenges related to the interoperability of electronic health records (EHRs) or electronic medical records (EMRs). EHRs and EMRs have slightly different practical uses but they have common characteristics and refer to an electronic form of health/medical records [6]. The terms are therefore used interchangeably in this work. This paper first discusses existing interoperability frameworks for EHRs/EMRs, identifying inadequacies in order to establish the need for an alternative framework.

The paper then proposes a novel framework to address existing interoperability challenges, especially those related to data exchange, privacy, and security. The framework was designed using a bottom-up approach, which consisted of examining existing interoperability frameworks to identify their inadequacies to determine the requirements for a novel and improved framework. The novel framework aims to achieve improved efficiency compared to past frameworks and is proposed to be implemented within a single legal jurisdiction; therefore, legal interoperability is not considered in this work.

1.2. Existing Interoperability Frameworks

An interoperability framework establishes rules and guidelines to enable different components or systems to work together to achieve interoperability. This section discusses existing interoperability frameworks for EHRs/EMRs in chronological order. The eHealth European Interoperability Framework (eEIF) constitutes a blueprint developed to effectively address the interoperability and standardization challenges within Europe's eHealth sector [7]. It was developed based on the foundations of the Antilope project and embodies a refinement of the broader European Interoperability Framework (EIF) to cater exclusively to the dynamic and evolving eHealth landscape [8]. At its core, the eEIF is designed to bolster the provision of European public services by cultivating an environment conducive to smooth interoperability that goes beyond both geographic and sectoral boundaries. The main purpose of the eEIF is to establish a universal framework and shared definition that systematically dissects interoperability challenges and eliminates eHealth-centric resolutions across the European Union landscape. The refined interoperability model in the eEIF consists of six levels: (i) legal and regulatory; (ii) policymaking; (iii) care execution; (iv) applications; (v) IT infrastructure; (vi) and information exchange.

Each level represents various aspects and stakeholders involved in achieving interoperability in the eHealth domain. The eEIF also provides a template for describing high-level use cases and realization scenarios, which helps in the provision of a consistent set of descriptions of and solutions to problems. Overall, the eEIF is a valuable tool for implementers and purchasers deploying eHealth systems, enhancing interoperability in the eHealth domain. It offers a common language and framework for addressing interoperability challenges and improving the delivery of eHealth services across Europe. The eEIF is dated and employs technical standards that have limitations and are difficult to implement. The current research aims to develop an alternative framework that focuses on the use of modern technologies and different standards that are easier to implement.

An interoperability framework was proposed by [9], with a focus on granting patients total control over their data and regulating how hospitals and healthcare organizations access such data. The framework leverages blockchain security and prioritizes network consensus, relying on proof of structural and semantic interoperability for consensus. While the framework achieved some success, it exhibited certain limitations. The inconsistent use of healthcare terminology among institutions posed challenges in interpreting and comprehending the shared data of patients and participating organizations. Standardizing this terminology emerged as a crucial challenge, as this impacts semantic interoperability within the framework.

Additionally, while the approach eliminated the need for a single, centralized source of trust, it introduced new security concerns due to the distributed nature of the blockchain network. Ensuring data privacy and protection from cyber-attacks remains a critical concern. Moreover, achieving a consistent view of patient records across the data-sharing network became problematic due to the distributed data sources and potential conflicts in data updates. As the number of participants and the volume of data increase, maintaining the scalability and performance of the Blockchain network will represent significant system performance challenges [10–12]. This research proposes an alternative framework that addresses the aforementioned limitations, including implementing a semantic mechanism for deriving the meaning and interpretation of standard data and prioritizing access control implementation to provide more robust data security.

The authors of [13] presented an interoperability framework that utilizes blockchain technology to ensure the privacy and security of patients' medical records in an interoperable environment. They proposed a blockchain-based framework named Ancile to facilitate secure, interoperable, and efficient access to medical records by patients, providers, and third parties while safeguarding patients' sensitive information. Ancile utilizes smart contracts in an Ethereum-based blockchain to enhance access control and data obfuscation, incorporating advanced cryptographic techniques for heightened security. While successful in achieving its intended objectives, the framework faces fundamental challenges related to scalability and the cost of storing data on blockchain platforms, rendering it unsuitable for nationwide deployment. Scalability issues and the associated costs of using blockchain technology make it impractical to implement on large-scale interoperable platforms, as has been noted by several authors, such as [14–17]. The current study proposes an alternative framework, addressing these challenges and emphasizing scalability and higher security measures.

An innovative access control framework was proposed by [18]. It focused on safeguarding the privacy of Personal Health Record (PHR) data during emergencies. This framework was built on permissioned blockchain technology, specifically utilizing the Hyperledger Fabric and Hyperledger Composer playground for evaluation. Through their experiments, the researchers demonstrated that the proposed framework ensures the secure sharing of PHR data, incorporating important features such as auditing, immutability, and emergency access control policies. This framework has limitations regarding latency and performance traits (related to scalability) that are inherent in the Hyperledger-based (blockchain) approach. The current research aims to overcome these limitations through the use of scalable technologies and therefore provide a more efficient and effective solution for handling PHR data within a healthcare ecosystem.

A conceptual framework was proposed by [19], aimed at enhancing decision-making processes within healthcare facilities in Tanzania through the implementation of EHRs. The paper establishes six propositions that underscore the role of EHRs' interoperability in supporting effective decision-making. It addresses the existing inconsistencies in EHR implementation and emphasizes the potential of interoperability to bridge these gaps and improve decision-making outcomes. The framework proposed in the paper emphasizes the collaborative potential of interoperable EHRs among healthcare professionals, facility managers, and policymakers, enabling shared decision-making. Furthermore, the framework highlights the importance of information exchange between policymakers and healthcare facility managers to create an environment conducive to efficient healthcare delivery. Despite its promising potential, the proposed interoperability conceptual framework for Tanzanian healthcare facilities exhibits certain limitations. It lacks applicability beyond the Tanzanian context, and the practical challenges associated with its implementation, encompassing technical, financial, and regulatory aspects, are not thoroughly addressed. Also, data security and privacy concerns, which are critical, are inadequately addressed. The current research seeks to propose an alternative framework that addresses the limitations discussed above.

In the study by [20], an interoperability framework was proposed to address the privacy challenges in sharing and storing EHRs. The study focused on introducing a framework named PbDinEHR, which focused on Privacy by Design (PbD) mechanisms, distributed data storage, and sharing in the context of EHRs. To showcase the framework's capabilities, the researchers developed a Patient Record Management System (PRMS), providing user interfaces for patients and healthcare providers. They also implemented a distributed file system and two permission blockchain networks using the Interplanetary File System (IPFS) and Ethereum blockchain, respectively, to ensure transparency and security when sharing patients' medical files with various healthcare providers. Despite these promising features, the PbDinEHR framework exhibits certain limitations.

Firstly, it lacks support for the right of erasure, a critical aspect defined in the General Data Protection Regulation (GDPR) that ensures privacy protection. Moreover, the frame-

work's security measures could be further enhanced by incorporating a robust encryption tool. Additionally, the level of user control provided by the framework is limited, and its scalability beyond the study's scope is questionable. To overcome these shortcomings, the current research proposes an alternative framework implementing progressive resistance against data breaches, employing dynamic data-masking techniques, and utilizing transparent database encryption. These measures are intended to address the identified limitations and strengthen the framework's overall effectiveness and security.

The DEPLOYR interoperability framework, which was proposed by [21] at Stanford University (USA), offers a swift solution for deploying custom real-time machine learning models into EMRs. It serves as a technical tool to facilitate the seamless deployment and monitoring of researcher-created clinical ML models within widely used EMR systems. The framework aims to establish best practices for machine learning (ML) deployment and bridge the existing gap in model implementation. While this framework has been influential in shaping the current research, it has certain limitations that render it unsuitable for nationwide interoperability. Notably, it is tailored to integrate with Stanford Health Care's EMR vendor, necessitating further customization for institutions using different EMR systems. As a result, its replication in other locations is challenging. DEPLOYR relies on data from Stanford University's common data model for model training, which may not be feasible or applicable to all settings. Moreover, it supports the APIs of the common FHIR standard for interoperability to comply with U.S. regulatory mandates, but this might require upgrades to accommodate a broader range of clinical ML applications with diverse data modalities, creating additional challenges. Furthermore, the framework's applicability is constrained by its dependency on specific data models and EMR systems, demanding further customization and adaptation for use in different environments. These limitations need to be carefully considered when considering its implementation beyond its original context. Considering the above, the current research aims to propose an alternative framework that addresses the discussed limitations, making the framework more suitable for nationwide interoperability.

An API-led integration framework was introduced by [22], aiming to improve the interoperability of patient health information amongst healthcare organizations. This framework is designed to maintain rigorous data privacy and security standards throughout its implementation. Central to its philosophy is the acknowledgment of the need for API integration to achieve the smooth and secure flow of data within the healthcare sector, facilitating the seamless exchange of data and functionality among various applications. The framework comprises a well-structured, three-tier architecture, with components that prioritize scalability, real-time capabilities, and orchestration. Emphasizing the potency of API-led connectivity, this framework has significant benefits, notably the reusability of the APIs, which contribute to the efficient development of its applications. In light of this, this research utilizes APIs to facilitate communication between disparate systems.

1.3. The Need for a Novel Conceptual Interoperability Framework for EHR

This work argues for a new conceptual interoperability framework to tackle the various challenges associated with achieving both semantic and technical interoperability in EHRs while preserving privacy and security. According to [23], a conceptual framework serves as a roadmap that helps conceptualize and organize work by connecting various ideas, concepts, and theories within the field of study, which, in this case, is the interoperability of EHRs. A conceptual framework is a structural foundation through which researchers endeavor to elucidate the inherent progression of the phenomenon under investigation [24]. A conceptual framework elucidates the interplay between the core concepts of a study. Its logical arrangement facilitates a visual representation, offering a tangible depiction of the interconnectedness of the ideas within the study [25]. It functions as the researcher's roadmap for delving into the research problem, outlining the path that is to be navigated. Through an integrated lens, the conceptual framework provides a comprehensive perspective on the studied issue, harmonizing various aspects into a coherent whole [26].

A conceptual framework substantially aids the researcher in meticulously defining and specifying the concepts pertinent to the study's problem [27]. Conceptual frameworks are aptly characterized as either "graphical or in a narrative form, showing the key variables or constructs to be studied and the presumed relationships between them" [28]. A conceptual framework provides a coherent and organized structure that guides the researcher's exploration, articulation, and understanding of the complex interplay among variables and constructs inherent to the research topic.

Interoperability fosters efficient healthcare delivery. Healthcare professionals can access vital patient information quickly and securely, streamlining the decision-making process and facilitating faster treatment interventions, as noted by [29]. In previous studies, many frameworks have been proposed, and some were partially able to address some of the challenges associated with the interoperability of EMRs/EHRs. Many limitations of existing interoperability frameworks (as discussed in Section 1.2) will be addressed in the proposed framework.

There is a need for a novel conceptual framework that takes a holistic approach to interoperability (incorporating security and privacy mechanisms) and aids in making accurate medical diagnoses using real-time access to patients' EHRs, formulating timely treatment plans, and ultimately improving patient outcomes. It has been argued that establishing standardized protocols, robust security measures, and governance frameworks are essential steps toward achieving seamless interoperability while safeguarding patient data privacy and security [30]. Only through these concerted efforts can healthcare systems fully realize the benefits of interoperability, ultimately leading to better patient care, improved outcomes, and enhanced population health, as reiterated by [31].

1.4. Requirements for a New Conceptual Interoperability Framework

Based on the related frameworks, discussed in Section 1.2 and other existing research, several key requirements for an efficient conceptual interoperability framework can be put forward, as follows:

- (a) **Modern and Scalable Technology:** Interoperability frameworks should utilize modern and scalable technologies to ensure that they can manage a large volume of data and participants without compromising performance. This includes avoiding single points of failure, as these can lead to significant downtime [32,33].
- (b) **Data Privacy and Security:** Ensuring the privacy and security of patient data is paramount. The framework must have robust mechanisms for access control, data obfuscation, encryption, and compliance with data protection regulations such as the UK DPA (GDPR) and the US Health Insurance Portability and Accountability Act (HIPAA) [34].
- (c) **Standardized Terminology:** The consistent use of standardized healthcare terminology is crucial for successful data sharing and interpretation. Addressing the challenges of inconsistent healthcare terminology is essential for achieving semantic interoperability.
- (d) **Flexibility and Adaptability:** The framework should be adaptable to different healthcare settings and EHR systems. It should support various data modalities and allow for customization to accommodate diverse clinical applications as well as diverse input and output formats [35].
- (e) **Support for Right of Erasure:** Compliance with data protection regulations like GDPR and HIPAA, including the right of erasure, should be part of the framework. It should provide users with control over the data that have been captured and processed [36].
- (f) **Progressive Resistance against Data Breaches:** The framework should implement measures like dynamic data-masking techniques and transparent database encryption to actively resist data breaches [36].
- (g) **Reusability of APIs:** An API-led integration approach should focus on creating reusable APIs. This contributes to efficient application development and data exchange among healthcare organizations [37,38].

- (h) **Real-Time Capabilities:** Frameworks should prioritize real-time data exchange capabilities to support immediate decision-making processes and provide up-to-date information [37].
- (i) **Compatibility:** A well-structured architecture with orchestration capabilities should be integral to the framework, ensuring that different components can work harmoniously despite their differences. This will also ensure that legacy systems can be integrated into the conceptual framework [21].
- (j) **Practical Applicability beyond the Original Context:** The framework should be designed with the ability to be implemented beyond its original context or region. It should address various technical, semantic, and regulatory concerns [38].

In conclusion, the above requirements should be incorporated into any new interoperability framework to address the limitations observed in the existing frameworks, which are critiqued in the above. The next section proposes a new framework that could better serve the needs of a wide range of healthcare systems.

2. The TASIPPS Conceptual Framework

This paper proposes the “Technical and Semantic Interoperability, Preserving Privacy and Security” (TASIPPS) conceptual framework to address multiple aspects of the previously discussed interoperability challenges by leveraging the strengths of several existing technologies in a novel way, in addition to incorporating new technologies. The main existing technologies that are used include the Service-Oriented Architecture (SOA), Fast Healthcare Interoperability Resources (FHIR), and Security Assertion Markup Language (SAML), to ensure a holistic, robust, and comprehensive interoperability solution. New technologies that are developed include an AI module that enables network monitoring and security, and a semantic interoperability module incorporating a novel medical (disease) ontology. The TASIPPS conceptual framework consists of six major components/modules, as illustrated in Figure 1: a Middleware server module; a semantic interoperability module; a privacy module; a security module; and the policy module.

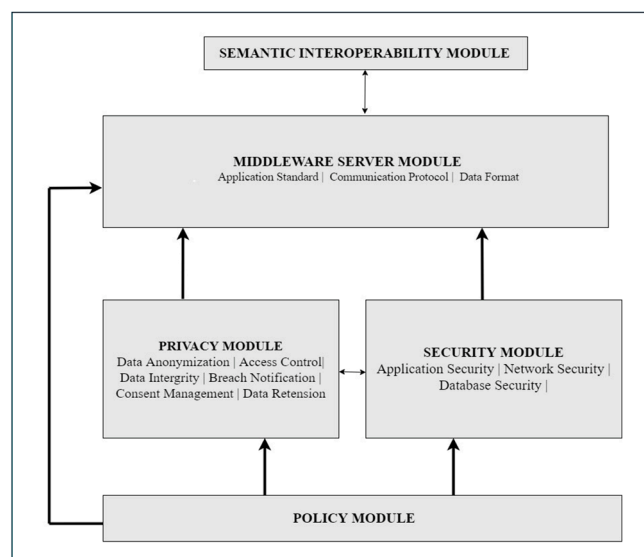


Figure 1. The TASIPPS Framework showing the components of the TASIPPS framework.

The framework components are described in greater detail in the next section.

2.1. The TASIPPS Framework Components

2.1.1. The Middleware Server Module

Technical interoperability pertains to the seamless communication and interaction between hardware/software components, systems, and platforms, facilitating machine-to-

machine connectivity [3]. This form of interoperability involves the utilization of standardized communication protocols and the necessary infrastructure to support these protocols' functioning. The focus of technical interoperability is ensuring efficient data exchange, allowing diverse machines and systems to interact cohesively within a connected ecosystem. Figure 2 shows the various components that make up the Middleware server module of the TASIPPS framework.

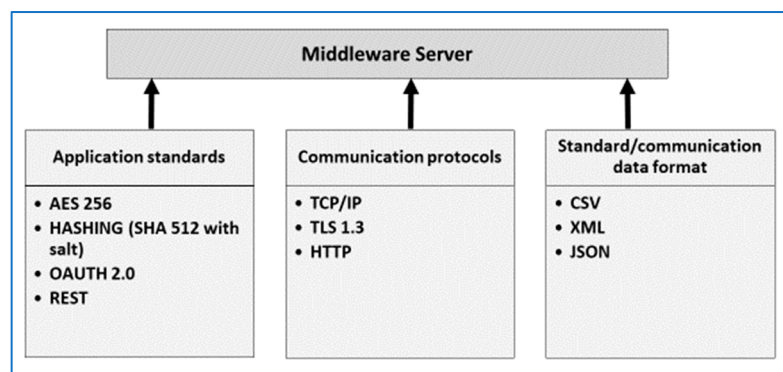


Figure 2. The Middleware server module's components.

Figure 2 presents the application standards, communication protocols, and the common data format that will be utilized within this framework. The components are explained below.

Application standards: The application standards defined within this framework set parameters and associated values to constrain the connecting systems technology in terms of performance or other features. The suggested AES 256 encryption is used for a range of encryption needs, including wireless networks and secure online transactions. The importance and suitability of this encryption model, because it is difficult for hackers to circumvent, were discussed by [39].

The extensive hash value of SHA-512 enhances its resistance to attacks, surpassing other hash functions in terms of security; as a result, SHA-512 is acknowledged as a potent, resilient, and swift hashing algorithm [40].

OAuth 2.0 permits restricted user data access, including access upon the expiration of authorization tokens. This capability enables data-sharing among users without the necessity of disclosing personal details. Furthermore, its implementation is simplified while also delivering enhanced authentication strength, as reiterated by [23].

The framework incorporates REST (Representational State Transfer) APIs, which have been recommended as the best way to facilitate interoperability due to their flexibility, allowing for the use of a variety of data formats [41]. A notable aspect of REST APIs is their flexibility [42]. REST APIs liberate data from being bound to resources or methods, allowing them to adeptly manage a variety of call types, offer diverse data formats, and seamlessly evolve in structure through the skillful incorporation of hypermedia. This makes REST APIs very suitable for the proposed framework.

2.1.2. The Semantic Interoperability Module

The semantic interoperability module is a subsection of the TASIPPS framework. It is positioned as an intermediary between disparate EHR systems, avoiding a central point of access that would be vulnerable to attacks. This placement ensures that data flow securely between systems without creating a single point of failure, enhancing both security and reliability. The various subcomponents of the module are explained below.

Adaptation of FHIR: The proposed solution to achieving interoperability does not utilize common technical interoperability standards such as openEHR or FHIR due to the need for participating hospitals to obtain new systems and other implementation costs to conform to these standards. It was also noted by [43] that the associated cost of

implementation, inconsistencies in the various versions, and variations in vendors during their implementation, amongst other factors, do not allow for common standards (such as openEHR or FHIR), which would provide the final answer to the interoperability challenge. Figure 3 captures the flow of traffic and how the EHR systems connect to the central database and the semantic interface.

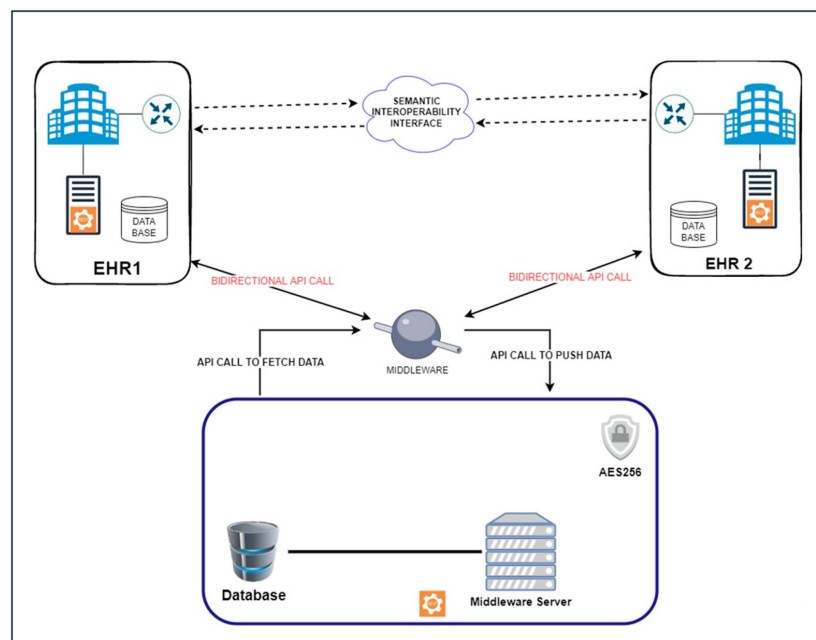


Figure 3. The semantic interoperability module and traffic flow.

The diagram in Figure 3 captures the two EHR systems that connect to the central database and the semantic interoperability interface. Both EHR systems connect to the central database and share basic patient information with the center, as depicted above. The EHR systems then connect to the semantic interface through API calls to fetch and push data. The proposed framework represents an advancement in interoperability through the forging of seamless connections between two distinct EHR systems—EHR1 and EHR2. At its core lies a sophisticated central database, designed to transcend traditional data silos and cultivate a holistic repository of patient information. By systematically populating this central database with essential but limited details, such as patient names, contact information, affiliated hospitals, and attending physicians, the framework sets the stage for a paradigm shift in healthcare data management. A pivotal feature of this framework is its bilateral connectivity, facilitated through the robust Application Programming Interfaces (APIs) between EHR1 and EHR2. This strategic interoperability not only allows for the exchange of data but also provides a novel approach to semantic interoperability.

The mechanics of the bidirectional data flow between EHR1 and EHR2 are orchestrated through a dedicated Semantic Interoperability Interface, which is integrated into the framework's architecture. This interface acts as a gatekeeper, regulating access to patient data between the two EHR systems. When a physician from EHR1 seeks patient information from EHR2, they engage with the Semantic Interoperability Interface, necessitating the input of secure login credentials. This process ensures a stringent verification of the user's identity and authorization status, fortifying the overall security of the interoperability ecosystem. The same process is replicated when a physician from EHR2 seeks data from EHR1, cementing the bidirectional nature of the interoperability framework.

Security is a paramount consideration in the implementation of this framework, with a robust array of access control mechanisms forming the vanguard. Users, whether from EHR1 or EHR2, are assigned predefined access rights contingent on their roles and responsibilities. This meticulous access control architecture ensures that sensitive

patient information is exclusively accessible to authorized personnel, mitigating the risk of unauthorized data exposure. Additionally, encryption protocols are systematically deployed to ensure data security during transmission, adding a layer of protection against potential data breaches.

Furthermore, the framework prioritizes the security of the interconnected EHR systems. Each EHR, when initiating a connection or data request through the central interface, undergoes a strict authentication process. The interface prompts the user to input secure credentials, validating both their identity and authorization status. Simultaneously, the interface ensures the legitimacy of the originating system, safeguarding against any malicious system or user activities. This two-fold authentication mechanism guarantees the integrity of data exchanges, providing an additional layer of security at the point at which a connection is initiated. As stated earlier, the framework employs the AES256 encryption method. In essence, the framework not only secures the data during transmission but also rigorously authenticates and authorizes every connection attempt, enhancing the overall security of the interoperability ecosystem.

How Semantic Interoperability Is Achieved

The semantic search process begins with the retrieval of vectorized data from a specialized database. This database contains vectorized representations of diseases and symptoms from each of the connected prototype systems. The vector index dimension of 1536 was used in this work. The vectorization process involves converting raw text data into numerical vectors using techniques like word embedding, which captures the semantic meaning of the text. In this work, the open-source AI model OpenAI's text-embedding-3-small was utilized to generate these vector embeddings. This model was chosen for its ability to produce high-quality, semantically rich vector representations at a lower cost. The text embedding created by this model is stored in a vector database, such as PG Vector, which facilitates efficient mathematical operations and comparisons during the search process. The choice of model and vector index length is optimized to enhance the relevance of the search results. Longer vector indexes, such as 1536 (as used in this work), provide a more detailed representation of the text and are associated with increased relevance in search outcomes. Figure 4 captures the various steps involved in the vectorization used in this work. By selecting appropriate models and vector index lengths, the system can improve the accuracy and effectiveness of the semantic search process.

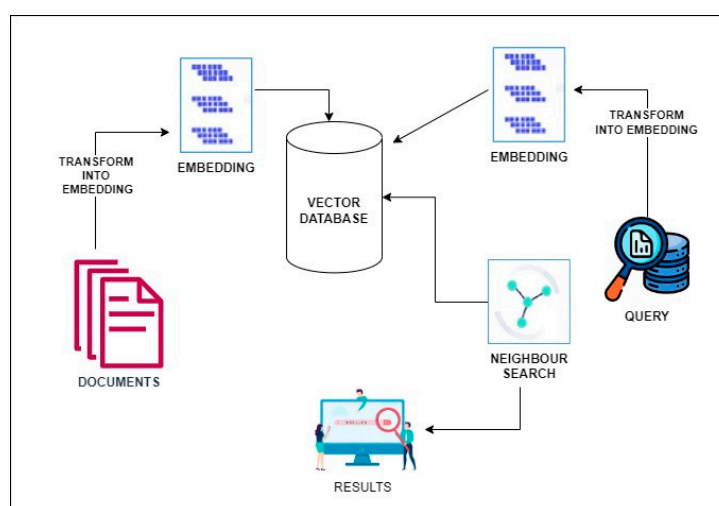


Figure 4. Vectorization flow (semantic search process).

The primary advantage of using a vectorized database over traditional ontology-based approaches lies in its ability to capture complex semantic relationships between medical terms without the need for exhaustive manual curation. Ontologies require extensive effort

to create and maintain, as they depend on predefined relationships and categories, which can be limiting and are prone to becoming outdated. In contrast, vectorized databases automatically learn and represent the semantic nuances of medical data through training on large datasets. This not only reduces the workload associated with manual updates but also enhances the flexibility and scalability of the system. By embedding the medical terminologies and their descriptions into a vector space, the system can leverage elastic semantic search capabilities to understand and retrieve relevant medical records based on the context of the search queries. This approach ensures more accurate and contextually relevant search results, ultimately improving the interoperability and usability of EHRs across different healthcare platforms.

When a requesting hospital initiates a search for a patient's medical history from the interoperability platform, it triggers the semantic search process. The requesting hospital (Hospital A) seeks to view the patient's medical history, which is stored in another hospital's (Hospital B) system. To facilitate this, the semantic search mechanism converts the patient's diagnosis and other relevant medical information from Hospital B's terminology into a format or terminology that Hospital A's system can understand and work with. Upon receiving the search request, the system first takes the search query and converts it into its own vector representation. This is achieved using the same OpenAI text-embedding-3-small model that was used to vectorize the data in the database. This conversion ensures that both the query and the stored medical data are represented in the same vector space, making meaningful comparisons possible.

With the vector representation of the search query in hand, the system performs a cosine similarity search to determine the relevance of the vectorized data to the search query. Cosine similarity measures the cosine of the angle between two vectors. This metric reflects how similar the vectors are in terms of their direction in the vector space, focusing on the orientation rather than the magnitude, which highlights the semantic closeness between the query and the stored data. The vector representation of the search query is compared with the vector representations of all data entries in the vector database. The system calculates the cosine similarity score for each comparison, indicating the degree of similarity between the query and each data entry. The results are then ranked based on their similarity scores, with higher scores indicating greater relevance to the query.

The system retrieves the top three most relevant results based on their similarity scores. These results contain information from across all connected hospitals, including Hospital B. The system then filters these results to ensure that the information returned is relevant to Hospital A, focusing on the specific needs of the querying system. As part of the filtering process, the system translates the patient's diagnosis and other relevant medical information from Hospital B's terminology into a format that Hospital A's system can understand. This step ensures that the medical information is not only relevant but is also comprehensible to the healthcare professionals at the requesting hospital.

The most relevant results from the semantic search are then returned to the requesting system at Hospital A. This process ensures that healthcare professionals have access to pertinent patient medical history in familiar terminology, enabling them to make accurate medical diagnoses, formulate timely treatment plans, and ultimately improve patient outcomes.

2.1.3. The Privacy Module

The privacy module within the framework is a critical component, designed to safeguard the confidentiality and individual rights of users regarding their personal information. This module addresses the ever-growing concerns surrounding data privacy, ensuring that the framework's operations adhere to stringent privacy regulations and the best practices laid out in the GDPR (UK/EU) and HIPAA (USA), which served as guidelines for this framework. By implementing robust privacy measures, the framework not only instills confidence in its users but also demonstrates a commitment to regulatory compliance, ethical data handling, and user-centric design. Figure 5 captures the sub-components of the privacy module within the framework.

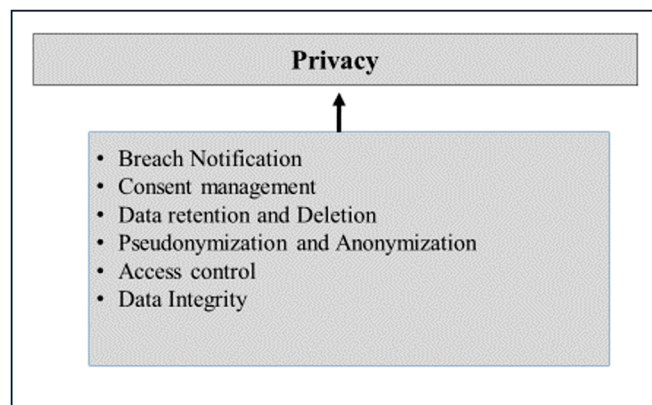


Figure 5. Sub-components of the privacy module of the TASIPPS framework.

Figure 4 shows the six (6) components that make up the privacy module. Together, these components achieve privacy; they are discussed in detail below.

Pseudonymization and Anonymization: Pseudonymization and anonymization are mandated by the GDPR Art 25 [44]. Pseudonymization is the process of identifying entities associated with privacy-sensitive data and replacing them with credible alternatives [45]. The incorporation of pseudonymization helps to improve the privacy of the health records [46]. In the works of [47,48], pseudonymization was used effectively; the original texts were replaced with synonyms and some lexical substitutes in placeholders to conceal them. In their privacy-preserving framework, [49] proposed the use of pseudonymization to achieve maximum privacy. Anonymization, on the other hand, involves removing personal identifiers from data to preserve the identity of the person or entity that the data have been collected about. The work of [50] utilized a combination of pseudonymization and anonymization to serve as an additional protection for the EHRs that were collected in their work. This work proposes anonymization and pseudonymization at the database level to conceal any personally identifiable patient data.

Data Access Controls: This encompasses the regulation and administration of data entry and access by employing specialized security mechanisms to guarantee the confidentiality, integrity, and availability of the data [51]. Data access controls are essential for maintaining data security and to ensure compliance with the data protection regulations enshrined in the GDPR (Art 5(f)) and HIPAA 45 CFR Part 164, Subpart C. This framework employs data access control mechanisms to ensure the privacy of patients' health records. This framework makes use of role-based access control, which grants access to data based on the role of the user. With this proposed framework, when a connected facility attempts to access a patient's medical history, a notification is sent to the patient prompting jim/her of the request. The steps that take place before patient authorization are explained as follows:

- A notification is sent to the patient explaining the query.
- The patient can review the query and either approve or deny the request.
- Access is only granted if the patient explicitly approves the request.
- If the patient does not approve the request, the system will log the denial and notify the requesting party that access has been denied.

This is depicted in Figure 6.

As depicted in Figure 6, the patient receives a notification indicating a request has been initiated to view their medical history. This notification will also indicate the name of the facility and will contain an option to grant or decline the request.

Data Integrity: Data integrity within the proposed framework encompasses maintaining the accuracy, consistency, and reliability of data across their entire lifecycle (GDPR Art 5). Data integrity ensures that information remains unaltered and dependable from its initial input through the storage, processing, and retrieval stages. In the context of this frame-

work, data integrity plays a pivotal role in upholding the credibility of the healthcare data that will be exchanged and managed within the system. This holistic approach to data integrity involves multiple strategies. It includes mechanisms such as version control, which keeps track of data modifications over time, ensuring a clear historical record of changes. Encryption techniques (AES256) are applied to secure the data during both the transmission and storage phases, fortifying their protection against unauthorized access. Hashing algorithms and HMAC (Hash-Based Message Authentication Code) protocols are employed to guarantee that data in transit remain unmodified and untampered, with real-time alerts configured to signal any potential breaches. Maintaining data integrity also encompasses a comprehensive review of access control procedures. Rigorous authentication and authorization protocols are established, ensuring that only authorized individuals are able to interact with data. Notably, all alterations or modifications will be meticulously documented and subject to approval before implementation, bolstering accountability and traceability. By seamlessly integrating these strategies, the framework ensures data integrity. This, in turn, underpins the reliability of the healthcare data, fostering an environment of trust, precision, and security throughout the system's operations.

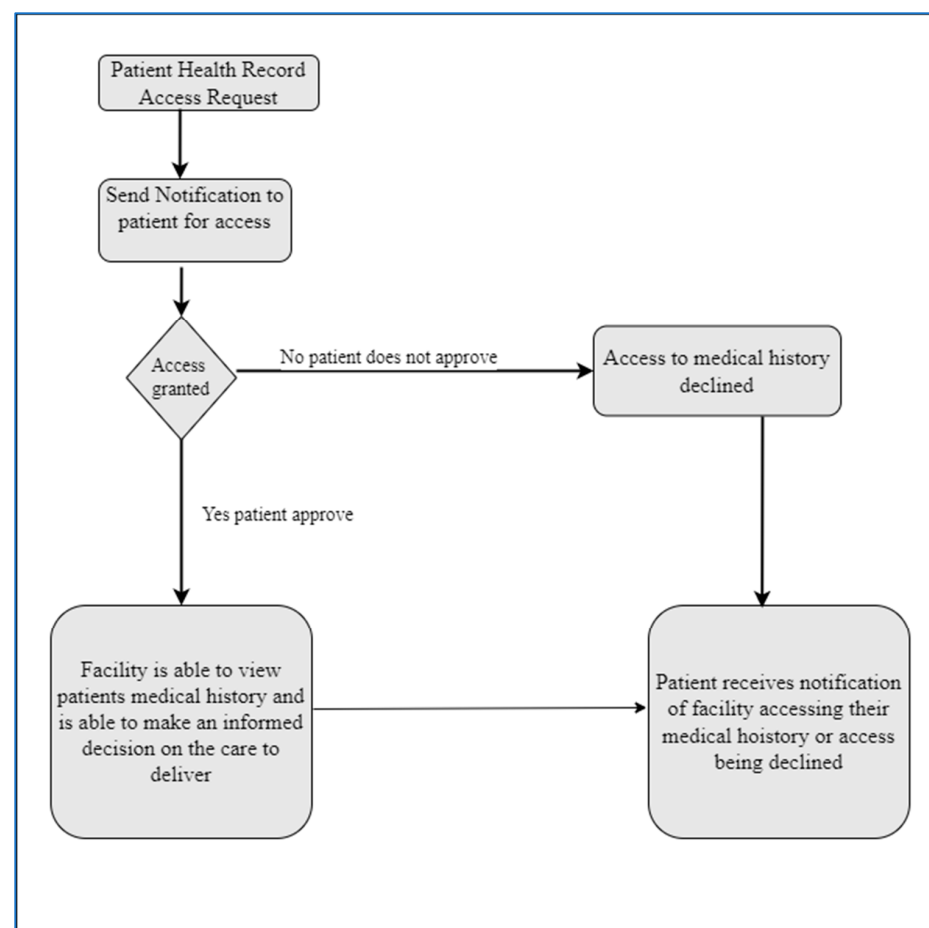


Figure 6. How patients grant and decline access to their data.

Data Retention and Deletion: Ensuring proper data retention and deletion is crucial for maintaining compliance with regulations, protecting privacy, and managing the lifecycle of data within the proposed framework. The retention and deletion of data will be guided by the storage limitation principle (Art 5(1) (e)) of the GDPR and other industry best practice guides. Within the policy module, the retention policies for the different data classifications are outlined. In this module, data classification is implemented to differentiate between sensitive data, important data, and non-sensitive data. This framework implements auto-

mated triggers on the various data classifications and initiates the deletion of data once the defined retention period expires. The framework also implements cryptographic erasure to ensure that deleted data cannot be restored. This ensures consistency and reduces the risk of human errors.

Consent Management: The framework implements an explicit opt-in mechanism where individuals actively provide their consent before their data are collected or processed, as mandated by Art. 7 of the GDPR. This is achieved through checkboxes and online forms. The proposed framework offers granular consent options that allow individuals to choose which specific portions of their EHR data they are comfortable sharing and for what purposes. This initiative empowers the patient to control the extent of the data sharing. There is also a straightforward process that enables individuals to withdraw their consent at any time. The framework incorporates a centralized system to document consent. This system stores information about who provided the consent, when it was provided, and for what purpose(s). Due to the various classifications of data, a prompt is presented for subjects to re-confirm their consent if their data usage changes.

Breach Notification: Implementing breach notifications requires a combination of technologies to ensure timely and accurate communication with affected individuals. This framework incorporates email notifications and system alert flags to notify participants of breaches. Within the framework’s user interface, web alerts are incorporated, which appear when users log in. These deliver breach notifications and valuable information immediately upon login. The GDPR mandates that the data protection authority must be promptly informed in the event of a system breach (Art 33) and the subjects of the data must also be informed if there is a risk to their rights and freedoms (Art 34).

2.1.4. The Security Module

This module manages the security aspect of the framework, which is critical in the sharing and exchanging of EHRs. The GDPR in (Art 5(1) (f)) states that personal data must be “processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures” This informs some of the actions undertaken to achieve security within the proposed research. Figure 7 shows the three components of the security module of the framework. They are application security, network security, and database security.

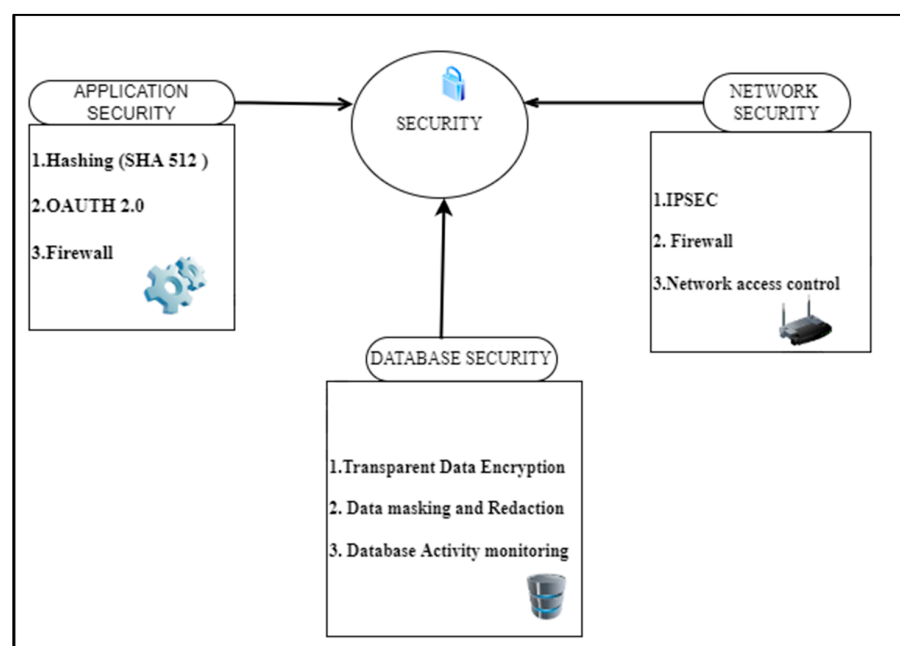


Figure 7. Components of the security module.

As illustrated in Figure 7, these three components are part of the security provisions needed to protect against attacks on the EHR systems, and form part of the interoperability system. The components are discussed further below.

Application Security

Within the proposed framework, a pivotal component is the application security layer, which is designed to enforce the security of the prototypes that are instrumental to the framework's functionalities. Application security measures are strategically employed to safeguard these prototypes, ensuring their integrity, confidentiality, and availability in the face of modern-day cyber-attacks, potential threats, and vulnerabilities. Incorporating SHA-512, OAuth 2.0, and strategically positioned firewalls, the application security layer functions as a safeguarding stronghold for the prototypes within the framework. These measures collectively bolster data integrity, control access, and mitigate risks, ensuring that the prototypes remain fortified against a diverse range of security challenges. As the backbone of the framework's security architecture, the application security layer plays an instrumental role in upholding the confidentiality, integrity, and availability of the prototypes and the sensitive data they manage.

Network Security

This component is geared towards safeguarding the foundation of the proposed framework. This is essential to the comprehensive security approach of the proposed framework, and a fundamental layer that ensures the protection and resilience of the entire network infrastructure upon which the framework is built. The implementation of robust network security measures is paramount to suppressing or eliminating potential threats, mitigating vulnerabilities, and maintaining the overall integrity of the framework's operations.

The network security module forms a resilient shield for the framework's operational environment by incorporating IPsec, Network Access Control, and fortified firewalls alongside sophisticated IDS/IPS. These measures collectively enhance data protection, secure communications, and bolster the framework's overall resilience against modern cyber threats. As the bedrock of the framework's security infrastructure, the network security module plays an instrumental role in safeguarding the integrity and continuity of operations across the interconnected parties.

Database Security

The database security subcomponent, a crucial facet of the overarching security module, stands as the sanctuary in which critical data reside. Its purpose is to ensure the impervious security of the data stored within the database, thereby maintaining its confidentiality, integrity, and availability. The implementation of a robust database security framework is pivotal to blocking or frustrating any potential breach attempts, preserving data privacy, and maintaining the unwavering trust of stakeholders.

The combination of Transparent Data Encryption (TDE), data masking, redaction, and Database Activity Monitoring (DAM) used within the database security subcomponent forges a resilient bastion for the data entrusted to the framework. These measures collectively uphold the sanctity of the data by fortifying their confidentiality, ensuring controlled access, and enabling a rapid response to potential threats. As the repository of sensitive information, the database security subcomponent stands as an unwavering bulwark against the diverse array of risks that seek to compromise the framework's most valuable asset—its data.

2.1.5. The Policy Module

The policy module within this framework is dedicated to governing and regulating various facets of system operations and data management. Its core purpose revolves around the formulation, enforcement, and administration of policies that safeguard the ethical, legal, and secure utilization of healthcare data within the framework proposed in

this study; these policies will be implemented and assessed later in this research. As [52] aptly noted, the “interoperability of EHRs is inevitably bound with data protection issues because of the processing of personal data” and, as such, policies must be put in place to ensure compliance with guiding principles such as the GDPR or HIPAA.

Consequently, the establishment of policies is imperative to ensure adherence to legal frameworks such as the UK/EU GDPR and the US HIPAA. The policies recommended in this work draw inspiration from the GDPR, HIPAA, and other industry best practices. The work was also inspired by the European Commission-issued Recommendation (EU) 2019/243 of February 2019, which is a comprehensive guide for achieving both technical and semantic interoperability while upholding the privacy and security of patient data. The policy module in this study aspires to follow this guidance by proposing a set of policies that will allow for the realization of privacy-preserving technical and semantic interoperability with robust security measures.

The following policies are implemented in the framework: the Compliance Monitoring Policy; Change Management Policy; Disaster Recovery and Business Continuity Policy; Data Consent Revocation Policy; Data Retention and Deletion Policy; Audit Logging Policy; Error Handling and Reporting Policy; Interoperability Testing Policy; Identity and Access Management Policy; and Consent Management Policy. The primary objective of the policy module is to establish a robust system that ensures adherence (by all stakeholders) to the (defined) interoperability standards and regulations governing EMRs. These policies are guided by the standards presented by [53], which advocate for consistent system monitoring.

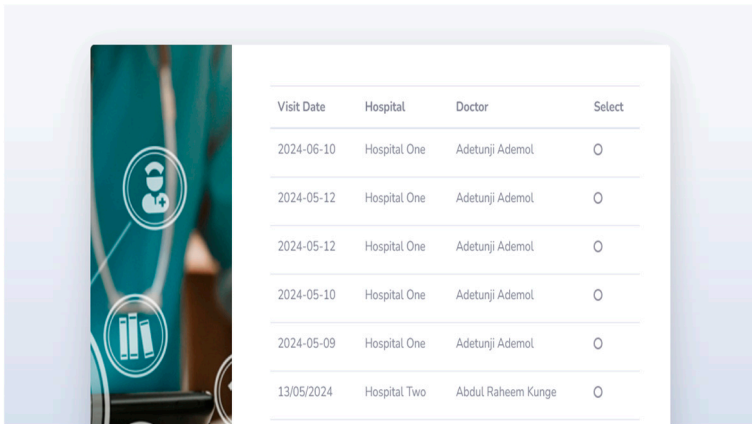
2.2. Case Study of the TASIPPS Framework

The TASIPPS framework was implemented in a system consisting of a central (interoperability) platform and two different EMR prototypes. A specific case study simulation, demonstrating the utilization of the TASIPPS framework, was successfully conducted during the testing. In this scenario, two simulated healthcare institutions with different EHR prototypes were integrated using the TASIPPS framework. The framework enabled seamless data exchange, ensuring that the medical records from one hospital were accurately interpreted and accessible to the other hospital in real-time. The semantic interoperability module played a crucial role in translating healthcare terminologies between the systems, avoiding any misinterpretation of patient data.

The necessary steps in accessing a patient’s medical history using the TASIPPS framework are as follows (see also Figure 8):

1. A doctor initiates query for patient history: During a consultation, if the doctor at Hospital A needs to review a patient’s medical history, stored by Hospital B, they initiate a query request to the central platform. The doctor’s role-based access control (RBAC) permissions are verified within Hospital A’s system to confirm they are authorized to make this request.
2. Request sent to central platform: The request (from Hospital A) is securely transmitted to the central platform, which acts as a mediator between the two connected prototype (hospital) systems. The central platform identifies the patient’s unique ID and prepares to fetch the patient’s medical records from both Hospital A (current) and Hospital B (connected).
3. Verification of doctor’s role: The central platform checks the RBAC policies of both systems to ensure that a user who is a doctor is making the request, adhering to the security protocols of each institution. This RBAC verification helps maintain the data access restrictions, allowing only qualified healthcare practitioners to access patient information.
4. Display of patient’s medical history: The central platform retrieves a list of the patient’s previous visitations from both Hospital A and Hospital B. The list includes details such as the visit date, hospital name, attending doctor’s name, and any relevant

- clinical notes. This information is presented in a consolidated view on the doctor's interface, allowing for a quick overview of the patient's history across institutions.
5. Patient consent request via OTP: Once the doctor selects a specific medical record to view, the central platform triggers a consent request to the patient's registered phone number. An OTP (one-time password) is sent to the patient, along with a secure link that allows them to approve or decline the data view request.
 6. Patient consent approval/denial: The patient receives the OTP and link, allowing them to verify the access request. By entering the OTP and selecting "Approve" or "Decline," the patient controls the sharing of their medical information, in compliance with privacy regulations.
 7. At this stage, the central platform ensures semantic interoperability by aligning the medical terminology and data structures across Hospital A and Hospital B. This alignment allows for data from disparate EMR systems to be accurately interpreted and presented in a consistent format on the doctor's interface. By standardizing terminologies and data models (see Section 2.1.2), the central platform ensures that the medical information from both hospitals is meaningful and accessible, providing the doctor with a unified view of the patient's medical history.
 8. Access granted to the doctor (upon approval): If the patient approves the request, the central platform grants the doctor access to view the selected medical record. The doctor can then review the patient's full details, which may contain critical information for the ongoing treatment.
 9. Audit logging for compliance: the central platform logs the entire transaction, including the identities of the requesting doctor, the patient's approval or denial, the time of access, and the specific records accessed. This audit trail helps ensure accountability and compliance with healthcare privacy/data protection regulations.



| Visit Date | Hospital | Doctor | Select |
|------------|--------------|--------------------|-----------------------|
| 2024-06-10 | Hospital One | Adetunji Ademol | <input type="radio"/> |
| 2024-05-12 | Hospital One | Adetunji Ademol | <input type="radio"/> |
| 2024-05-12 | Hospital One | Adetunji Ademol | <input type="radio"/> |
| 2024-05-10 | Hospital One | Adetunji Ademol | <input type="radio"/> |
| 2024-05-09 | Hospital One | Adetunji Ademol | <input type="radio"/> |
| 13/05/2024 | Hospital Two | Abdul Raheem Kunge | <input type="radio"/> |

Figure 8. Screenshot showing a list of the patient's medical history.

In the case study, the privacy and security mechanisms, including AES-256 encryption and role-based access controls, were fully functional, ensuring that only authorized personnel could access sensitive patient information. The consent management system was also successfully tested, allowing for patients to approve or deny access to their medical records before the data exchange took place.

This case study, supported by the test results, showcases the framework's ability to facilitate interoperability, enhance data security, and comply with privacy regulations. It proves the system's effectiveness in real-world settings, making it a valuable solution to the challenges regarding the interoperability of healthcare.

2.3. Evaluation and Discussion

The TASIPPS framework was evaluated by comparing it to existing frameworks using various criteria relevant to the achievement of interoperability. The comparison table (Table 1) compares the proposed framework with the related works discussed in Section 1.2.

Table 1. Framework comparison table.

| Criteria | eEIF | Blockchain-Based (Sharma et al., 2021 [31]) | Ancile | Hyperledger-Based (Access Control) | Tanzanian EHR Framework | PbDinEHR | DEPLOYR | API-Led Integration | TASIPPS |
|--|------|---|--------|------------------------------------|-------------------------|----------|---------|---------------------|---------|
| Semantic Interoperability | Yes | No | No | No | Yes | Yes | No | No | Yes |
| Technical Interoperability | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Reusability | No | No | No | No | No | No | No | Yes | Yes |
| Scalability | No | No | No | No | No | No | No | Yes | Yes |
| Compliance to Standards | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Consent Management (Privacy) | No | Yes | Yes | Yes | No | No | No | Yes | Yes |
| Access Control (Security) | Yes | Yes | Yes | Yes | No | No | No | Yes | Yes |
| Network Security | Yes | Yes | Yes | Yes | No | No | No | Yes | Yes |
| Identity and Access Management (Security) | Yes | Yes | Yes | Yes | No | No | No | Yes | Yes |
| Threat Detection and Prevention (Security) | No | Yes | Yes | Yes | No | No | No | Yes | Yes |
| Legal Interoperability | Yes | No | Yes | Yes | No | No | No | Yes | Yes |
| Privacy | Yes | Yes | Yes | Yes | No | No | No | Yes | Yes |

The evaluation of the TASIPPS framework in the comparison table (Table 1) highlights its ability to comprehensively meet key interoperability challenges through modern technologies and robust security measures. The evaluation criteria are explained below.

1. **Semantic Interoperability:** the framework excels by utilizing standardized healthcare terminologies, ensuring consistent and accurate data interpretation across systems. This addresses a major limitation seen in other frameworks.
2. **Technical Interoperability:** The framework is highly adaptable, allowing for seamless integration with various EHR systems and clinical applications, making it suitable for diverse healthcare environments.
3. **Reusability:** With its modular architecture, the framework supports the reuse of components, which enables flexibility and reduces system redundancy. This reusability enhances system maintenance and expansion.
4. **Scalability:** The framework is built on a cloud-based infrastructure with dynamic resource allocation and load-balancing, allowing the framework to scale efficiently as data volumes and workflow complexities grow.
5. **Compliance with Standards:** By leveraging widely accepted standards like SOA, FHIR, and SAML, TASIPPS ensures compliance, reducing the risk of obsolescence and maintaining compatibility with future systems.
6. **Consent Management:** The framework integrates comprehensive privacy controls, including consent management, to ensure that patients have control over their healthcare data, aligning with regulations like the GDPR and HIPAA.
7. **Access Control:** Through advanced mechanisms like OAuth 2.0-based authentication and authorization, TASIPPS ensures that only authorized personnel can access sensitive patient data, providing strong access control.
8. **Network Security:** The framework employs advanced encryption techniques such as AES-256 and SHA-512, maintaining high levels of security in terms of data transmission and storage, which ensures the protection of healthcare data.

9. **Identity and Access Management:** The framework provides robust identity and access management solutions to secure sensitive healthcare data, enhancing security across interconnected systems.
10. **Threat Detection and Prevention:** With built-in threat detection and prevention mechanisms, the framework safeguards healthcare data against cyber-attacks and breaches, ensuring a high level of system protection.
11. **Legal Compliance:** The framework also complies with legal frameworks by offering mechanisms for dynamic data masking and data erasure, ensuring adherence to privacy regulations like GDPR.
12. **Privacy:** Finally, the framework provides enhanced privacy features such as data obfuscation and masking, ensuring that sensitive patient data remain secure while ensuring compliance with key data protection regulations.

In comparison with other frameworks, the TASIPPS framework stands out for its holistic approach, integrating privacy, security, and interoperability into a cohesive solution. Its cloud-based infrastructure, combined with its advanced security measures and support for emerging technologies, ensures the framework remains scalable, future-proof, and adaptable to the evolving needs of data exchanges in healthcare. One possible limitation of the TASIPPS framework, which will be addressed in further work, is the complexity of implementing it across different regions, as variations in regional healthcare systems, regulations, and technological infrastructures may require further customization and adaptation.

3. Conclusions

This research proposed a new conceptual framework to ensure the interoperability of EHRs using a bottom-up approach. The TASIPPS framework streamlines access to comprehensive patient data for healthcare providers, enabling more informed and timely decision-making. This reduces administrative burdens, allowing healthcare professionals to focus on patient care. The enhanced semantic interoperability, powered by the semantic search and AI text-embedding components, ensures that data are presented consistently across different systems, minimizing the risk of misinterpretation. For patients, the TASIPPS framework improves the continuity of care by making health records easily accessible and transferable across providers, leading to more coordinated and personalized care with fewer delays and treatment errors.

A comparison of the framework with existing frameworks showed that the TASIPPS framework addresses key limitations in privacy, security, and scalability while providing enhanced interoperability across distinct healthcare systems, positioning it as a more comprehensive solution to modern healthcare needs. In summary, the TASIPPS framework is well-positioned to remain relevant and effective in the rapidly evolving healthcare landscape, offering long-term viability in diverse healthcare environments. Its scalability and adaptability make it suitable for large-scale and nationwide deployment, allowing for its seamless integration into existing systems at a comparatively low cost. By creating a user-friendly environment for both healthcare providers and patients, with security and privacy at the forefront, the TASIPPS framework ultimately leads to better healthcare outcomes, improved patient satisfaction, and an efficient, interoperable healthcare ecosystem for all stakeholders.

Author Contributions: Conceptualization, A.A. and C.G.; methodology, A.A. and C.G.; validation, A.A., C.G. and G.M.; formal analysis, A.A. and C.G.; investigation, A.A.; data curation, A.A.; writing—original draft preparation, A.A.; writing—review and editing, A.A., C.G. and G.M.; visualization, A.A., C.G. and G.M.; supervision, C.G. and G.M.; project administration, C.G. and G.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created for this article.

Acknowledgments: We are grateful for the ALERT Research Group in the Computer Science Department at Middlesex University (London, UK) for the nurturing support provided during this work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. IEEE. Standards Glossary. 2013. Available online: http://www.ieee.org/education_careers/education/standards/standards_glossary.html (accessed on 13 August 2024).
2. Young, P.; Chaki, N.; Berzins, V.; Luqi, L. Evaluation of middleware architectures in achieving system interoperability. In Proceedings of the 14th IEEE International Workshop on Rapid Systems Prototyping Proceedings, San Diego, CA, USA, 9–11 June 2003; pp. 108–116.
3. Reis, Z.S.N.; Maia, T.A.; Marcolino, M.S.; Becerra-Posada, F.; Novillo-Ortiz, D.; Ribeiro, A.L.P. Is there evidence of cost benefits of electronic medical records, Standards, or Interoperability in hospital information systems? Overview of systematic reviews. *JMIR Med. Inform.* **2017**, *5*, e7400. [CrossRef]
4. Abernethy, A.; Adams, L.; Barrett, M.; Bechtel, C.; Brennan, P.; Butte, A.; Faulkner, J.; Fontaine, E.; Friedhoff, S.; Halamka, J.; et al. The Promise of Digital Health: Then, Now, and the Future. *NAM Perspect.* **2022**, *6*, 108–116. [CrossRef] [PubMed]
5. World Health Organization. Digital Health and Innovation. 2024. Available online: <https://www.who.int/publications/m/item/digital-health-and-innovation> (accessed on 20 July 2024).
6. Shinozaki, A. Electronic Medical Records and Machine Learning in Approaches to Drug Development. In *Artificial Intelligence in Oncology Drug Discovery and Development*; IntechOpen: London, UK, 2020. [CrossRef]
7. Ntafi, C.; Spyrou, S.; Bamidis, P.; Theodorou, M. The legal aspect of interoperability of cross border electronic health services: A study of the European and national legal framework. *Health Inform. J.* **2022**, *28*, 146045822211287. [CrossRef] [PubMed]
8. Kouroubali, A.; Katehakis, D.G. The new European interoperability framework as a facilitator of digital transformation for citizen empowerment. *J. Biomed. Inform.* **2019**, *94*, 103166. [CrossRef] [PubMed]
9. Peterson, K.J.; Deeduvanu, R.; Kanjamala, P.; Mayo, K. A Blockchain-Based Approach to Health Information Exchange Networks. 2016. Available online: <https://www.semanticscholar.org/paper/A-Blockchain-Based-Approach-to-Health-Information-Peterson-Deeduvanu/c1b189c81b6fda71a471adec11cfe72f6067c1ad> (accessed on 13 August 2024).
10. Yang, H.; Yang, B. A Blockchain-Based Approach to the Secure Sharing of Healthcare Data. In Proceedings of the Norwegian Information Security Conference 2017, Oslo, Norway, 27–29 November 2017; pp. 100–111.
11. Lin, Q.; Wang, H.; Pei, X.; Wang, J. Food Safety Traceability System Based on Blockchain and EPCIS. *IEEE Access* **2019**, *7*, 20698–20707. [CrossRef]
12. Yan, X.; Wu, Q.; Sun, Y. A Homomorphic Encryption and Privacy Protection Method Based on Blockchain and Edge Computing. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8832341. [CrossRef]
13. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]
14. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [CrossRef]
15. Linn, L.A.; Koo, M.B. A Blockchain for Healthcare: The Solution to Trustworthy Health Data. Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. 2016. Available online: <https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf> (accessed on 20 July 2024).
16. Ivan, D. Moving toward a blockchain-based method for the secure storage of patient records. In Proceedings of the ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, MD, USA, 22–24 August 2016; pp. 1–11.
17. Brodersen, C.; Kalis, B.; Leong, C.; Mitchell, E.; Pupo, E.; Truscott, A. Blockchain Technology: Opportunities for Healthcare. Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. 2016. Available online: https://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf (accessed on 20 July 2024).
18. Rajput, A.R.; Li, Q.; Ahvanooy, M.T. A blockchain-based secret-data sharing framework for personal health records in emergency condition. *Healthcare* **2021**, *9*, 206. [CrossRef]
19. Mwogosi, A. Digital Transformation in Tanzania’s Healthcare Sector: A Systematic Review of Robust Electronic Health Records Systems’ Critical Success Factors. *Res. Sq.* **2023**. [CrossRef]
20. Semantha, F.H.; Azam, S.; Shanmugam, B.; Yeo, K.C. PbDinEHR: A Novel Privacy by Design Developed Framework Using Distributed Data Storage and Sharing for Secure and Scalable Electronic Health Records Management. *J. Sens. Actuator Netw.* **2023**, *12*, 36. [CrossRef]
21. Corbin, C.K.; Maclay, R.; Acharya, A.; Mony, S.; Soumya Punnathanam Thapa, R.; Kotecha, N.; Shah, N.H.; Chen, J. DEPLOYR: A technical framework for deploying custom real-time machine learning models into the electronic medical record. *J. Am. Med. Inform. Assoc.* **2023**, *30*, 1532–1542. [CrossRef] [PubMed]
22. Mishra, R.; Kaur, I.; Sahu, S.; Saxena, S.; Malsa, N.; Narwaria, M. Establishing three layer architecture to improve interoperability in Medicare using smart and strategic API led integration. *SoftwareX* **2023**, *22*, 101376. [CrossRef]

23. Singh, S. What Is a Conceptual Framework and How to Make It (with Examples). *Researcher Life*. 2023. Available online: <https://researcher.life/blog/article/what-is-a-conceptual-framework-and-how-to-make-it-with-examples/> (accessed on 19 September 2024).
24. Camp, W.G. Formulating and Evaluating Theoretical Frameworks for Career and Technical Education Research. *J. Vocat. Educ. Res.* **2001**, *26*, 27–39. [[CrossRef](#)]
25. Grant, C.; Osanloo, A. Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blue print for ‘House’. *Adm. Issues J. Connect. Educ. Pract. Res.* **2014**, *4*, 12–22. [[CrossRef](#)]
26. Liehr, P.; Smith, M.J. Middle Range Theory: Spinning Research and Practice to Create Knowledge for the New Millennium. *Adv. Nurs. Sci.* **1999**, *21*, 81–91. [[CrossRef](#)]
27. Luse, A.; Mennecke, B.; Townsend, A. Selecting a Research Topic: A Framework for Doctoral Students. *Int. J. Dr. Stud.* **2012**, *7*, 143–152. [[CrossRef](#)]
28. Miles, M.B.; Huberman, A.M. *Qualitative Data Analysis An Expanded Sourcebook*; Sage Publications: Thousand Oaks, CA, USA, 1994; Available online: <https://www.scirp.org/reference/referencespapers?referenceid=1423956> (accessed on 15 August 2024).
29. Christodoulakis, C.; Asgarian, A.; Easterbrook, S. Barriers to adoption of information technology in healthcare. In Proceedings of the 27th Annual International Conference on Computer Science and Software Engineering, Toronto, ON, Canada, 4–6 November 2019; pp. 66–75.
30. Spanakis, E.G.; Sfakianakis, S.; Bonomi, S.; Ciccotelli, C.; Magalini, S.; Sakkalis, V. Emerging and Established Trends to Support Secure Health Information Exchange. *Front. Digit. Health* **2021**, *3*, 636082. [[CrossRef](#)]
31. Sharma, P.; Borah, M.D.; Namasudra, S. Improving security of medical big data by using Blockchain technology. *Comput. Electr. Eng.* **2021**, *96*, 107529. [[CrossRef](#)]
32. Oikonomou, E.K.; Khera, R. Designing medical artificial intelligence systems for global use: Focus on interoperability, scalability, and accessibility. *Hell. J. Cardiol.* **2024**. [[CrossRef](#)]
33. Thantharate, P.; Thantharate, A. ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain. *Big Data Cogn. Comput.* **2023**, *7*, 165. [[CrossRef](#)]
34. Williamson, S.M.; Prybutok, V. Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare. *Appl. Sci.* **2024**, *14*, 675. [[CrossRef](#)]
35. López, D.M.; González, C.; Blobel, B. Ontology-based interoperability service for HL7 interfaces implementation. In *Seamless Care—Safe Care*; IOS Press: Amsterdam, The Netherlands, 2010; pp. 108–114.
36. Tikkinen-Piri, C.; Rohunen, A.; Jormanainen, I. EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies. *Comput. Priv. Data Prot.* **2018**, *34*, 134–153. [[CrossRef](#)]
37. Sultan, T. Compliance with the GDPR and HIPAA: A Comparative Study in Healthcare Sector. *J. Priv. Data Prot.* **2020**, *23*, 56–72.
38. *ISO/TR 20514:2005*; Health Informatics—Electronic Health Record—Definition, Scope and Context. ISO—International Organization for Standardization: Geneva, Switzerland, 2020. Available online: <https://www.iso.org/standard/39525.html> (accessed on 12 August 2024).
39. Selvapriya, E.S.; Suganthi, L. Design and implementation of low power Advanced Encryption Standard cryptcore utilizing dynamic pipelined asynchronous model. *Integration* **2023**, *93*, 102057. [[CrossRef](#)]
40. Wang, K.; Wu, X.; Wang, H.; Kan, H.; Kurths, J. New color image cryptosystem via SHA-512 and hybrid domain. *Multimed. Tools Appl.* **2021**, *80*, 18875–18899. [[CrossRef](#)]
41. IBM. What Is a REST API? | IBM. 2023. Available online: <https://www.ibm.com/topics/rest-apis> (accessed on 12 August 2024).
42. Palma, F.; Olsson, T.; Wingkvist, A.; Gonzalez-Huerta, J. Assessing the linguistic quality of REST APIs for IoT applications. *J. Syst. Softw.* **2022**, *191*, 111369. [[CrossRef](#)]
43. Itirra. What Is HL7? Advantages and Disadvantages Explained | Blog. 2023. Available online: <https://itirra.com/blog/hl7-advantagesdisadvantages/> (accessed on 24 June 2023).
44. Gdpr-text.com. Article 5 GDPR. Principles Relating to Processing of Personal Data | GDPR-Text.com. Available online: <https://gdpr-text.com/read/article-5/> (accessed on 15 August 2024).
45. Eder, E.; Wiegand, M.; Krieg-Holz, U.; Hahn, U. “beste grüße, maria meyer”—Pseudonymization of privacy-sensitive information in emails. In Proceedings of the Thirteenth Language Resources and Evaluation Conference, Marseille, France, 20–25 June 2022; European Language Resources Association: Marseille, France, 2022; pp. 741–752.
46. Ertmer, P.A.; Newby, T.J. Behaviorism, cognitivism, constructivism: Comparing critical features from an instructional design perspective. *Perform. Improv. Q.* **2013**, *26*, 43–71. [[CrossRef](#)]
47. Pierre, L.; Ildikó, P.; David, S.; Montserrat, B.; Lilja, Ø. Anonymization models for text data: State of the art, challenges and future directions. In Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers), Virtual Event, 1–6 August 2021; Association for Computational Linguistics: Stroudsburg, PA, USA, 2021; pp. 4188–4203.
48. Pilán, I.; Lison, P.; Øvrelid, L.; Papadopoulou, A.; Sánchez, D.; Batet, M. The Text Anonymization Benchmark (TAB): A Dedicated Corpus and Evaluation Framework for Text Anonymization. *Comput. Linguist.* **2022**, *48*, 1053–1101. [[CrossRef](#)]
49. Yue, Z.; Ding, S.; Zhao, L.; Zhang, Y.; Cao, Z.; Tanveer, M.; Jolfaei, A.; Zheng, X. Privacy-preserving time-series medical images analysis using a hybrid deep learning framework. *ACM Trans. Internet Technol. (TOIT)* **2021**, *21*, 1–21. [[CrossRef](#)]

50. Ross, G.M.S.; Zhao, Y.; Bosman, A.J.; Geballa-Koukoula, A.; Zhou, H.; Elliott, C.T.; Nielen, M.W.F.; Rafferty, K.; Salentijn, G.I.J. Best practices and current implementation of emerging smartphonebased (bio)sensors—Part 1: Data handling and ethics. *TrAC Trends Anal. Chem.* **2023**, *158*, 116863. [[CrossRef](#)]
51. Yuan, H.; Wang, Z.; Chen, Z.; Gong, Y.; Lu, J.; Hu, Y.; Li, L.; Qian, F. A Fine-Grained Access Control Method Based on Role Permission Management. In Proceedings of the 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballar, India, 29–30 April 2023. [[CrossRef](#)]
52. Bincoletto, G. Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union. *Data Policy* **2020**, *2*, e3. [[CrossRef](#)]
53. Oracle.com. Risk and Compliance. 2023. Available online: <https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/risk-and-compliance.htm> (accessed on 15 August 2024).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.