Article

Addressing the Interoperability of Electronic Health Records: Proposing the TASSIPS Framework

Adetunji Ademola [*] , Carlisle George [*] , Glenford Mapp Ezra

Posted Date: 6 August 2024

doi: 10.20944/preprints202408.0381.v1

Keywords: Interoperability; Electronic health records; Semantic; Security; Privacy; Healthcare Out-comes; Framework

Article

Addressing the Interoperability of Electronic Health Records: Proposing the TASSIPS Framework

Adetunji Ademola *, Carlisle George * and Glenford Mapp

Dept of Computer Science, Middlesex University, London (UK); aa4802@live.mdx.ac.uk (A.A.); c.george@mdx.ac.uk (C.G.); g.mapp@mdx.ac.uk (G.M.)

* 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 (EHR), 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 for electronic health records is saddled with challenges hindering efficient interoperability. Existing interoperability frameworks for EHR have failed to properly address many of these challenges relating to data exchange, security and privacy. To address these challenges, the TASSIPS framework is proposed as a comprehensive approach to achieving efficient interoperability. TASSIPS 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. TASSIPS offers a holistic and effective solution to healthcare interoperability challenges. An evaluation of TASSIPS via comparison with exicting frameworks concluded that it is an advancement in framework design for interoperability of EHR.

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

1. Introduction

Interoperability refers to two or more systems or applications sharing and utilizing information or data [18,40,53]. 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, ultimately advancing the overall quality of healthcare services [1]. Despite the numerous benefits, there are significant challenges related to 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 [50]. This long-term commitment underscores the importance of creating robust frameworks that address challenges related to interoperability of electronic health records (EHRs) or electronic medical records (EMRs). EHRs and EMRs have slightly different practical uses but they have common chracteristics and refer to health/medical records in electronic form [45]. The terms EHRs and EMRs are therefore used interchangeably in this work. This paper first discusses existing interoperability frameworks for EHRs/EMRs with a view to 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 related to data exchange, privacy and security. Finally the novel framework is evaluated by comparing it with existing frameworks using relevant criteria.

1.2. Existing Interoperability Frameworks

An interoperability framework establishes rules and guidelines to enable different componements or systems to work together to achieve interoperability. This section discusses existing interoperability frameworks for EHRs/EMRs based on chronological order.

The eHealth European Interoperability Framework (eEIF) constitutes a blueprint developed to effectively address interoperability and standardization challenges within Europe's eHealth sector [33]. It was developed based on the foundations of the Antilope project and embodies a refinement adapted from the broader European Interoperability Framework (EIF) to cater exclusively to the dynamic and evolving eHealth landscape [22]. 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 dissect interoperability challenges and eliminate eHealth-centric resolutions across the European Union landscape. The refined interoperability model in the eEIF consists of six levels: (I) Legal and regulatory; (ii) Policy making; (iii) Care execution; (iv) Applications; (v) IT infrastructure; (vi) and Information exchange. Each level represents different 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 problem descriptions and solutions. Overall, the eEIF is a valuable tool for implementers and purchasers to deploy eHealth systems and enhance 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 [36] with a focus on granting patients total control over their data and regulating how hospitals and healthcare organizations access such data. The framework leveraged blockchain security and prioritized network consensus, relying on proof of structural and semantic interoperability for consensus. While the framework showcased success, it exhibited certain limitations. The inconsistent use of healthcare terminology among institutions posed challenges in interpreting and comprehending shared data for patients and participating organizations. Standardizing terminology emerged as a crucial challenge, thereby impacting semantic interoperability within the framework. Additionally, while the approach eliminated 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 remained a critical concern. Moreover, achieving a consistent patient record view across the data sharing network became problematic due to distributed data sources and potential conflicts in data updates. As the number of participants and data volume increases, maintaining the scalability and performance of the Blockchain network will raise significant system performance challenges challenges [25,51,52]. This research proposes an alternative framework that addresses the aforementioned limitations including implementing semantic mechanism for standard data meaning and interpretation, and prioritizing access control implementation to provide robust data security.

The authors [10] 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 associated costs of blockchain that make them impractical to implement on large-scale interoperable platforms have been noted by several authors such as [3,6,20,26] .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 [39] focused on safeguarding the privacy of Personal Health Record (PHR) data during emergency situations. This framework is built on permissioned Blockchain technology, specifically utilizing Hyperledger Fabric and Hyperledger Composer playground for evaluation. Through their experiments, the researchers demonstrated that the proposed framework ensures secure data sharing of PHRs, incorporating important features such as auditing, immutability, and emergency access control policies. This framework has limitations regarding latency or performance traits (related to scalability) that are inherent in the Hyperledger-based (block chain) approach. The current research aims to overcome these limitations by use of scalable technologies and therefore the provision of a more efficient and effective solution for handling PHR data within a healthcare ecosystem.

A conceptual framework by [32] 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 EHR 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 practical challenges associated with 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 work seeks to propose an alternative framework that addresses the limitations discussed above.

In the study by [43], an interoperability framework was proposed to address 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 the 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 framework'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 may be 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 [9] 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 ML deployment best practices 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 exclusively with EMR software from Epic Systems, necessitating further customization for institutions using different EMR systems. As a result, its replication in other locations becomes challenging. DEPLOYR relies on data from Stanford'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. In light of the above, the current research aims to propose an alternative framework that addresses the limitations discussed, making it more suitable for nationwide interoperability.

An API-led integration framework was introduced by [31] , aiming to achieve 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 API integration as the solution for achieving smooth and secure flow of data within the healthcare sector, facilitating the seamless exchange of data and functionality among various applications. Within the framework lies the establishment of a well-structured three-tier architecture, comprising components that prioritize scalability, real-time capabilities and orchestration. Emphasizing the potency of API-led connectivity, this framework highlights the significant benefits, notably the reusability of APIs, which contribute to efficient application development. It's worth noting that the framework employs RESTful API, chosen for its inherent strengths and advantages. Nevertheless, the implementation of the proposed framework utilized FHIR and HL7 standards, which comes with acknowledged limitations and challenges. There are a couple of considerations to bear in mind with regards to the limitations of the proposed framework. The framework introduces a single point of failure, the Enterprise Service Bus (ESB), which serves as the central hub connecting all services. In the event of ESB downtime, communication between clients and services becomes impossible. Furthermore, the additional layer of indirection may potentially result in a decrease in the performance of client-service communication within the proposed framework. These aspects warrant careful consideration in its implementation. These flaws in communications should be addressed in any new framework where multiple communication tunnels are established between parties and does not have a single point of failure which can also affect performance.

1.3. Proposing a Novel Interoperability Framework for EHR

This work proposes a new conceptual (interoperability) framework to tackle the various challenges associated with achieving both semantic and technical interoperability of EHR while preserving privacy and security. According to [47], 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 defined as a structural foundation through which researchers endeavor to elucidate the inherent progression of the phenomenon under investigation [7]. A conceptual framework elucidates the interplay between the core concepts within a study. Its logical arrangement facilitates a visual representation, offering a tangible depiction of the interconnectedness of ideas within the study [16]. It functions as the researcher's roadmap for delving into the research problem, outlining the path 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 [24]. A conceptual framework substantially aids the researcher in meticulously defining and specifying the concepts pertinent to the study's problem [28]. 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" [30]. In essence, 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.

Achieving 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 [8]. From previous studies, many frameworks have been proposed and some have been partially able to address some of the challenges associated with interoperability EMRs. Many have limitations which will be discussed further below and addressed in the proposed framework.

The proposed conceptual framework takes a holistic approach to interoperability (incorporating security and privacy mechanisms) and aids in making accurate medical diagnoses due to 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 towards achieving seamless interoperability while safeguarding patient data privacy and security [48]. 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 [44]. This framework aims to achieve the latter and is proposed with the assumption of it being implemented within a single legal jurisdiction, therefore legal interoperability is not considered in this work.

1.4. Requirements for a Conceptual Interoperability Framework

Based on the related frameworks discussed in Section 1.1 above and other exiting research, several key requirements for an efficient conceptual interoperability framework can be deduced as follows:

- ***Modern and Scalable Technology*:** Interoperability frameworks should utilize modern and scalable technologies to ensure that they can handle a large volume of data and participants without compromising performance. This includes avoiding single points of failure, as they can lead to significant downtime **cf**. [10,36].
- ***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 US HIPAA cf. [39].
- ***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.
- ***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 [27].
- ***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 their data that has been captured and processed **cf**. [43].
- ***Progressive Resistance against Data Breaches*:** The framework should implement measures like dynamic data masking techniques and transparent database encryption to resist data breaches actively **cf**. [43].
- ***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 cf. [19,31].
- ***Real-Time Capabilities*:** Frameworks should prioritize real-time data exchange capabilities to support immediate decision-making processes and provide up-to-date information cf. [31].
- ***Compatibility*:** A well-structured architecture with orchestration capabilities should be integral to the framework, ensuring that different components can work harmoniously in spite of their differences. This will also ensure legacy systems can be integrated into the conceptual framework **cf**. [9].
- ***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 [19].

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

2.0. Proposing the TASIPPS Conceptual Framework

This paper proposes the "Technical and Semantic Interoperability Preserving Privacy and Security"(TASIPPS) conceptual framework to address multiple aspects of interoperability challenges previously discussed by leveraging the strengths of several existing technologies in a novel way in addition to incorporating new technologies. The main existing technologies 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 developed include an AI module which enables network monitoring and security, and also 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 below namely: semantic interoperability module, middleware server, privacy module, security module, AI module and the policy module.

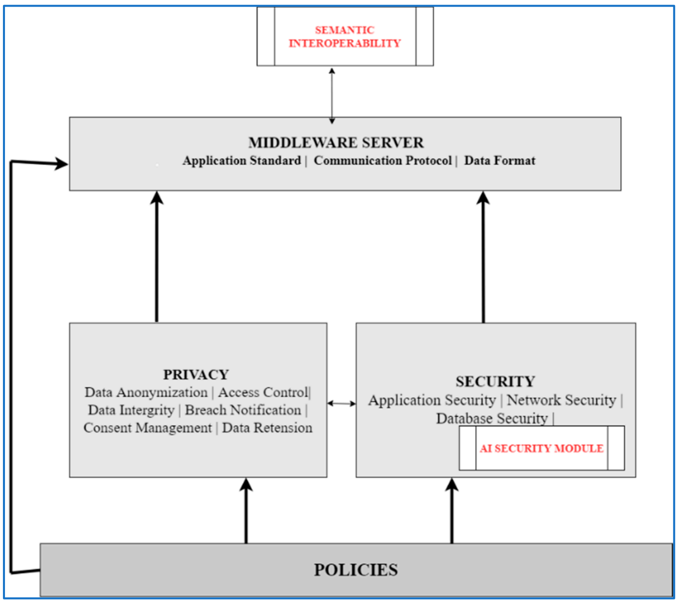
SEMANTIC INTEROPERABILITY
MIDDLEWARE SERVER
Application Standard | Communication Protocol | Data Format
PRIVACY
Data Anonymization | Access Control|
Data Intergrity | Breach Notification |
Consent Management | Data Retension
SECURITY
Application Security | Network Security |
Database Security |
AI SECURITY MODULE
POLICIES

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

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

2.1. TASIPPS Framework Components

2.1.1. Middleware Server Module

Technical interoperability pertains to the seamless communication and interaction between hardware/software components, systems, and platforms, facilitating machine-to-machine connectivity [49]. 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 to ensure efficient data exchange, allowing diverse machines and systems to interact cohesively within a connected ecosystem. Figure 2 below shows the various components that make up the technical interoperability module of the TASIPPS framework.

doi:10.20944/preprints202408.0381.v1

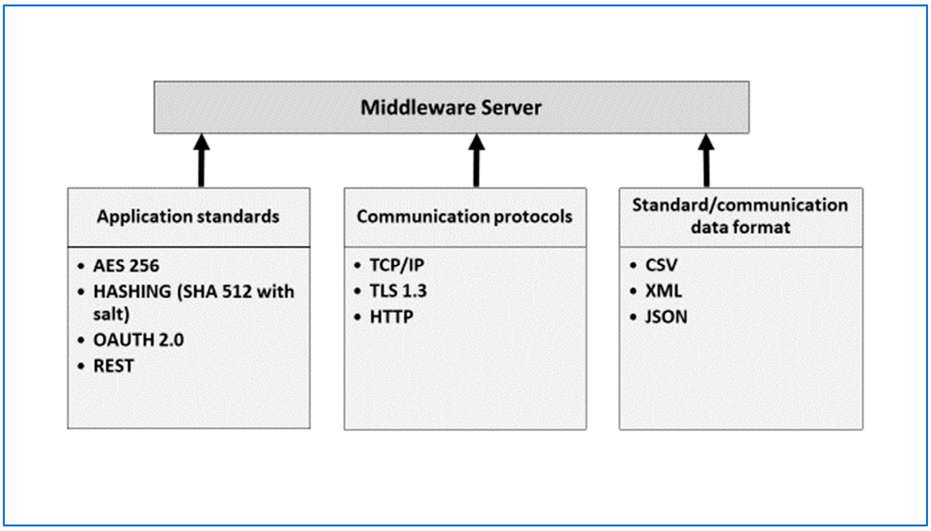

Figure 2. Middleware server components.

Figure 2 above captures 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 sets parameters and associated values to constrain the connecting systems technology in terms of performance or other features. The AES 256 encryption suggested is used for a range of encryption needs which includes wireless networks and secure online transactions. The importance of this model was echoed by [42] and reiterated the suitability of this encryption model because it is difficult for hackers to crack.

The SHA 512 is the hashing algorithm that this framework will employ due to its secured nature. It is mainly used to encrypt an input message to produce a fixed digest (hash value) which serves as a security feature for each message transmitted. The extensive hash value of SHA-512 enhances its resistance to attacks, surpassing other hash functions in security and as a result, SHA-512 is acknowledged as a potent, resilient, and swift hashing algorithm [23].

The OAuth 2.0 was selected due to its suitability for this framework to handle the authorization functionality enshrined in this framework. OAuth 2.0 permits restricted user data access, including access upon 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 [47] .

The framework incorporates REST (Representational State Transfer) APIs which have been recommended as the best way to facilitate interoperability due to its flexibility with a variety of data formats [17]. It was indicated that a notable aspect of REST APIs lies in its flexibility[35]. REST liberates data from being bound to resources or methods, allowing it 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 API very suitable for the proposed framework. REST API is an adaptation of the HTTP protocol, which is implemented in this work in a novel way not previously done by any of the concepts/prototypes mentioned earlier. The REST API represents a modern method (compared to SOAP and .NET) of facilitating communication between participants and the interoperability platform, to enable faster data queries and retrievals.

Communication protocols: This module handles the rules that have been formalized to handle the transmission and exchanging of data between the hospitals that are connected to the proposed platform which forms part of the framework. This framework employs the HTTP (hypertext transfer protocol), which is a highly familiar and widely recognized protocol, holds a distinct position as an integral element of the internet's framework. Functioning within the application layer. This protocol facilitates effective communication between web browsers and servers, constituting a pivotal conduit for data exchange within the digital the proposed interoperability platform which will facilitate connectivity between disparate systems.

Transmission Control Protocol (TCP) is also utilized in this framework. It is an essential facet of network communication and it serves the purpose of fragmenting data into discrete packets whiles rendering them amenable for transmission across networks. These packets are subsequently conveyed through the switches and routers and will undergo seamless dissemination to their intended recipients. This adds to the coherent functioning of data transmission mechanisms that the frame work proposes and seeks to achieve with the interoperability platform that has been proposed.

Parallel to TCP, the Internet Protocol (IP) serves as a complementary mechanism that partitions data into smaller units or packets, ensuring enhanced maneuverability within the network landscape. Diverging from TCP's role, IP operates as a pivotal instrument for the internet, orchestrating the intricate routing and addressing of data across diverse networks. In doing so, IP engenders the precise conveyance of data to its designated terminus, exemplifying its instrumental role in enabling accurate data delivery within the expansive digital terrain.

Standard/common data format: This part of the technical interoperability deals with the structure and representation of the data that will be exchanged. This will ensure consistency in the organization and encoding of the exchanged data and would allow for the disparate systems to be able to understand the exchanged data seamlessly. The framework employs JSON (JavaScript Object Notation) which is widely used for representing structured data in a human-readable format that is easy for both humans and machines to understand. The XML (eXtensible Markup Language) is a versatile markup language that allows for the definition of customized tags, enabling the representation of diverse types of data. The CSV (Comma-Separated Values) standard is also used for the data that will be generated and utilized for the AI algorithm. This will ensure compliance from all systems and make it easy for the AI module to process the input data.

2.1.2. Semantic Interoperability Module

The Semantic interoperability module is a subsection of the TASSIPS framework. The semantic module has been strategically positioned between the two connecting hospitals used for this test as a security measure and to avoid any single point of attack and failure of the system. This was also done to assuage any privacy and security concerns the participating hospitals would have about centralizing their patient data as a result of facilitating interoperability. 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 openEHR or FHIR, due to the need for participating hospitals to obtain new systems and undergo other implementation costs to conform to these standards. The approach taken in this work uses a combination of alternative technologies that allows legacy systems in hospitals to be used, and hence does not require the implementation of new hospital systems. It was also noted by [21] that the associated cost of implementation, inconsistency in the various versions and vendor variation during implementation amongst others, does not make common standards (such openEHR or FHIR) the total answer to the interoperability challenge. To establish robust semantic interoperability within the TASIPPS framework, a mapping table is meticulously designed which serves as a reference point. This strategic mapping table is the conduit that harmonizes diverse terminologies utilized by the interconnected prototype systems. The purpose is to forge a shared understanding and ensure the agreement of meaning or description for healthcare concepts exchanged. The figure below captures the flow of traffic and how the EHR systems connect to the central database and the semantic interface.

The above diagram Figure 3 captures the two EHR systems that connect to the central database and the semantic interoperability interface. Both of the EHR systems connect to the central database and share basic patient information to the center as depicted above. The EHR systems then connect to the semantic interface through API calls to fetch and to push data. The proposed framework represents an advancement in interoperability by forging 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 the bilateral connectivity facilitated through robust Application Programming Interfaces (APIs) between EHR1 and EHR2. This strategic interoperability empowers not only the exchange of data but also new approach in semantic interoperability. Going beyond simple data sharing, semantic interoperability ensures a shared understanding of medical information, harmonizing meaning and interpretation across disparate systems. This transformative aspect is integral to enhancing collaborative patient care and enabling a more comprehensive approach to healthcare decision-making.

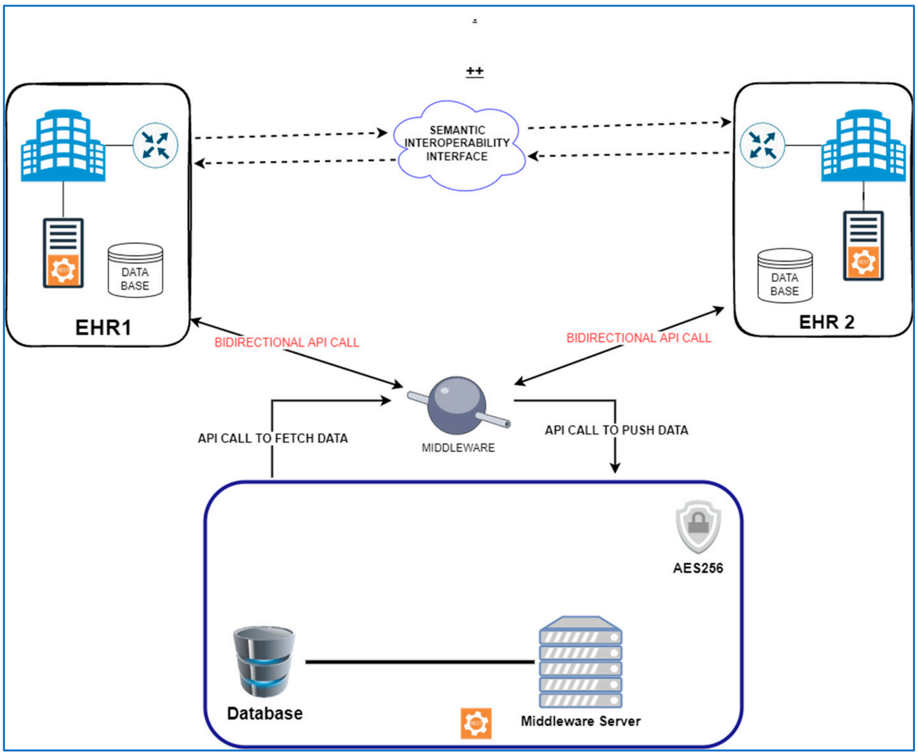

Figure 3. Semantic Interoperability Module and traffic flow.

The mechanics of bidirectional data flow between EHR1 and EHR2 are orchestrated through a dedicated Semantic Interoperability Interface which has been 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 reverse 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 an additional 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 of connection initiation. 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 posture of the interoperability ecosystem.

2.1.3. 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 vectorization process involves converting raw text data into numerical vectors using techniques like word embedding, which capture the semantic meaning of the text. For this work the open-source AI model was utilized, OpenAI's text-embedding-3-small, to generate these vector embedding. 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 are 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 search results. Longer vector indexes, such as 1536, provide a more detailed representation of the text and are associated with increased relevance in search outcomes. The Figure 4 below 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.

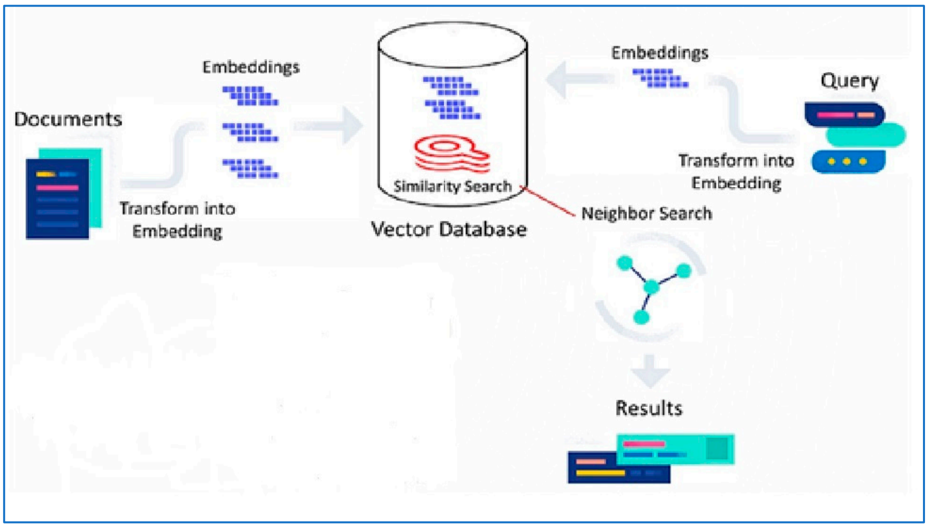

Figure 4. showing the vectorization flow.

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 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 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 previous 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 stored in another hospital's (Hospital B) system. To facilitate this, the semantic search mechanism aims to convert 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 vector representation. This is done 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 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. 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 also comprehensible to the healthcare professionals at the requesting hospital.

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

2.1.4. Privacy Module

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

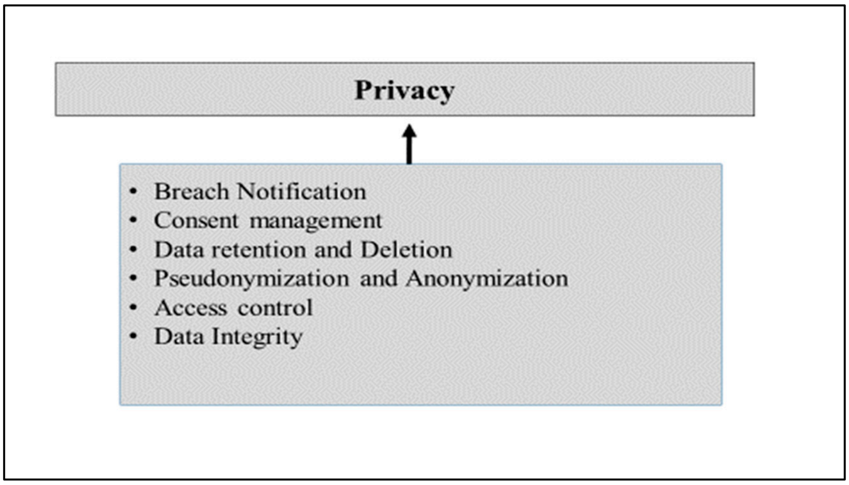

Figure 5. Sub-components of the Privacy module of the TASIPPS framework.

The figure above (Figure 5) shows the six (6) components that make up the privacy module. Together these components achieve privacy and are discussed in detail below.

Pseudonymization and Anonymization: Pseudonymization and Anonymization are mandated by the *GDPR Art 25* [15]. Pseudonymization is the process of identifying entities associated with privacy-sensitive data and replacing them with credible alternatives [11]. With this platform incorporating Pseudonymization, it helps to improve the privacy of the health records that will be processed or accessed through this platform [12]. In the works of [37] and [38], they used pseudonymization effectively and replaced the original texts in place holders with synonyms and some lexical substitutes to conceal the original texts. In their privacy preserving framework, [55] proposed the use of pseudonymization in the achievement of maximum privacy. Anonymization on the other hand has to do with removing personal identifiers from data to preserve the identity of the person or entity that data has been collected about. The work of [41] utilized a combination of pseudonymization and anonymization to serve as an additional protection to EHRs that was collected in their work. This work proposes anonymization and pseudonymization at the database level to conceal any personal identifiable data of patients.

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 data [54]. Data access controls are essential for maintaining data security and compliance with 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 patient's health records. This framework makes use of the 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 patients' medical history, a notification is sent to the patient prompting them of the request. The patient has the option to grant the access or decline. This is depicted in the Figure 6 below.

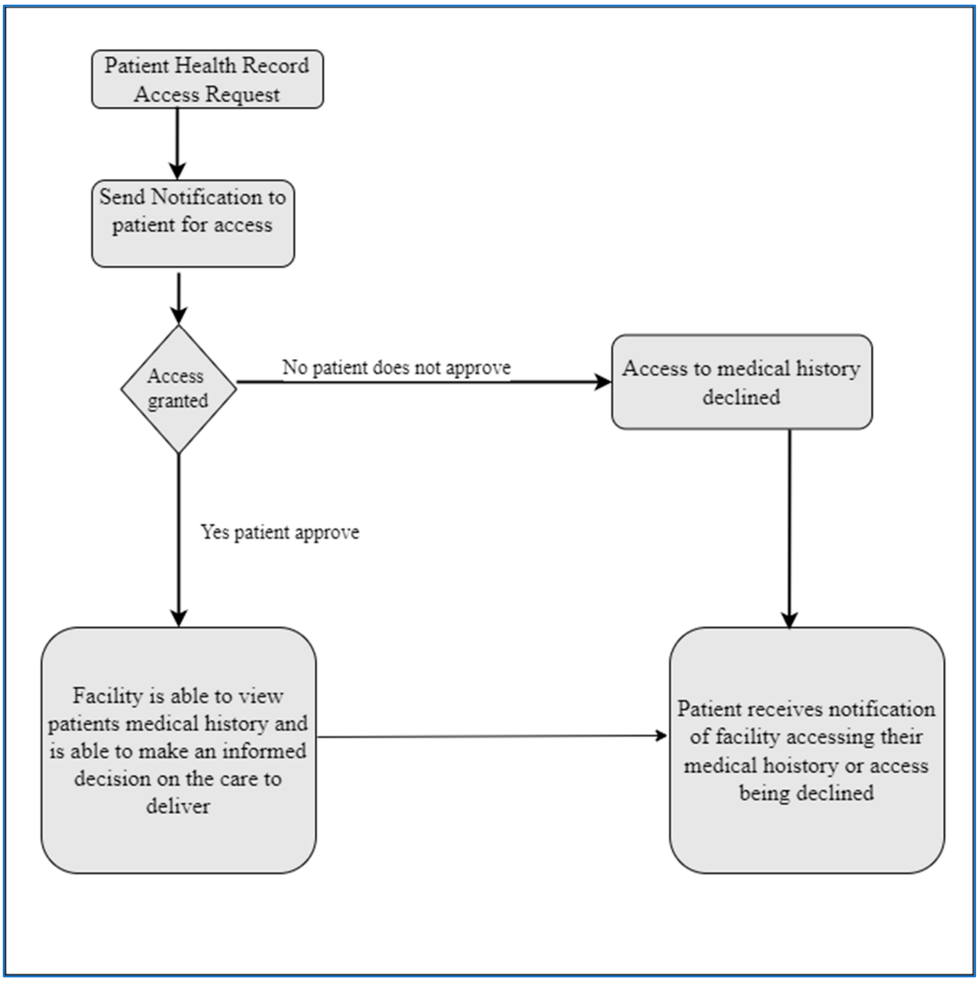
Patient Health Record Access Request
Send Notification to patient for access
Access granted
No patient does not approve
Access to medical history declined
Yes patient approve
Facility is able to view patients medical history and is able to make an informed decision on the care to deliver
Patient receives notification of facility accessing their medical hoistory or access being declined

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

From the above diagram (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 its entire lifecycle (GDPR Art 5(f)). Data integrity ensures that information remains unaltered and dependable from initial input through storage, processing, and retrieval stages. In the context of the framework, data integrity holds a pivotal role in upholding the credibility of 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 data during both transmission and storage phases, fortifying its protection against unauthorized access. Hashing algorithms and HMAC (Hash-Based Message Authentication Code) protocols are employed to guarantee that data in transit remains 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 will be established, ensuring that only authorized individuals possess the privilege 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 healthcare data, fostering an environment of trust, precision, and security throughout the system's operations.

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 data retention and deletion will be guided by the storage limitation principles (Art 5(1)(e)) of the GDPR and some other industry best practice guides. Within the Policy Module, policies are outlined to define the retention policies on the different data classifications. As part of this module, data classification is implemented to differentiate between sensitive data, important data and non-sensitive data. This framework implements automated 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 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 give their consent before their data is collected or processed as mandated by Art. 7 of the GDPR. This is done 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 data sharing. There is also a means to provide a straightforward process for individuals to withdraw their consent at any time. The framework incorporates a centralized system to manage records of consent. This system stores information about who provided consent, when it was given, and for what purposes. Due to the various classifications of data, a prompt is present 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 to appear when users log in. These deliver breach notifications and important information immediately upon login. The GDPR, mandates that both data protection authorities must be promptly informed in the event of a system breach (Art 33) and data subjects must be informed if there is a risk to their rights and freedoms. (Art 34).

2.1.5. Security Module

This module handles the security aspect of the framework which is very critical in the sharing and exchanging of EHRs. The GDPR (2019) 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 against 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 below shows the three components of the security module of the framework. They are application, network and database security.

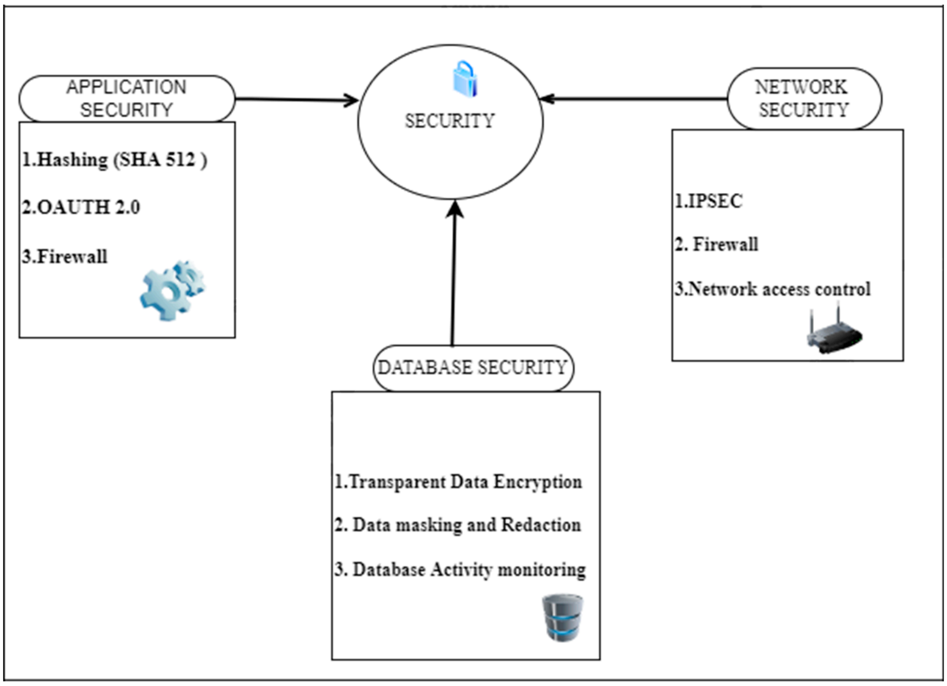

Figure 7. Components of the security module.

As illustrated in Figure 7 above, the three components are needed to have a formidable resistance against the attacks that EHR systems have been suffering in recent times. The components (Application Security, Network Security and Database Security) are discussed further below.

Application Security

Within the proposed framework, a pivotal component is the application security layer, designed to enforce the security posture of the prototypes that are instrumental in implementing the framework's functionalities. The 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.

Secure Hash Algorithm (SHA-512): One of the cornerstone security measures applied within the application security layer is the utilization of SHA-512. This is a robust cryptographic hash function. This hashing algorithm ensures the integrity of data by generating a fixed-size hash value unique to the input data. By implementing SHA-512, any alteration or tampering with the prototypes' data will result in a different hash value, immediately signaling potential breaches. This mechanism bolsters data integrity, rendering the prototypes resistance to unauthorized modifications.

OAuth 2.0 serves as another pivotal security measure woven into the application security framework. This authorization framework ensures controlled access to resources while preventing unauthorized access. OAuth 2.0 facilitates secure authentication and authorization processes, allowing the prototypes to grant access only to authorized users or systems. By employing OAuth 2.0, the framework strengthens the prototypes' defenses against unauthorized entry, ensuring that only authenticated and authorized entities interact with sensitive data and functionalities.

Firewalls: To provide comprehensive protection, the application security layer employs robust firewall mechanisms. These firewalls act as barriers between the prototypes and potential external threats, regulating incoming and outgoing network traffic. By enforcing access controls, the firewalls prevent unauthorized access, data breaches, and cyberattacks. They form a critical shield against threats that attempt to compromise the prototypes' security through network 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

doi:10.20944/preprints202408.0381.v1

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 on. 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.

IPsec (Internet Protocol Security): is at the core of the network security module and the strategic utilization of IPsec, a suite of protocols designed to secure Internet Protocol (IP) communications. IPsec creates a secure channel for data transmission, encryption and authentication of network packets to prevent eavesdropping, tampering, and unauthorized access. By leveraging IPsec, the framework establishes a secure tunnel through which data is transmitted, shielding it from potential interception or manipulation. This encryption-based mechanism bolsters the confidentiality and integrity of data in transit, ensuring that critical information remains private and untampered.

Network Access Control (NAC): An essential facet of the network security strategy is Network Access Control (NAC), a solution that governs access to the network based on predefined security policies. NAC enforces stringent authentication and authorization mechanisms, allowing only authorized devices and users to connect to the network. By implementing NAC, the framework ensures that only legitimate entities gain entry, preventing unauthorized access attempts and enhancing overall network security.

Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS): The network security module further encompasses the integration of potent firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) which have been specified in the requirements chapter of this document. Firewalls act as vigilant gatekeepers, monitoring and filtering incoming and outgoing traffic based on defined rules. They shield the network from malicious attempts, preventing unauthorized access and potential data breaches. Complementing firewalls, IDS/IPS function as advanced sentinels, actively identifying and responding to suspicious activities or intrusion attempts. By swiftly detecting and neutralizing potential threats, IDS/IPS contribute to a proactive defense against attacks.

Incorporating IPsec, Network Access Control, and fortified firewalls alongside sophisticated IDS/IPS, the network security module forms a resilient shield for the framework's operational environment. These measures collectively enhance data protection, secure communications, and bolster the framework's overall resilience against a 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 where critical data resides. Its purpose is to ensure the impervious security of the data stored within the database, thereby maintaining the confidentiality, integrity, and availability of the framework's database. 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.

Transparent Data Encryption (TDE): Central to the database security strategy is the adoption of Transparent Data Encryption (TDE), a transformative mechanism that encrypts data at rest within the database. TDE ensures that sensitive information remains unintelligible to unauthorized access attempts, even if physical storage media are compromised. By enveloping data in an impregnable cryptographic shield, TDE fortifies the confidentiality of data against breaches, mitigating the risk of unauthorized exposure.

Data Masking and Redaction: Augmenting the database security landscape, data masking and redaction techniques are employed to safeguard sensitive data during queries and reports. Data masking obfuscates sensitive information, such as personal identifiers, while still allowing

doi:10.20944/preprints202408.0381.v1

operational use of the data. Redaction, on the other hand, selectively hides or replaces sensitive content from database results, and ensures that only authorized personnel can access complete information. These techniques strike a balance between operational utility and data protection, preventing unnecessary exposure while maintaining functional data access.

Database Activity Monitoring (DAM): A linchpin of the database security subcomponent is the strategic integration of Database Activity Monitoring (DAM). This technology actively monitors and audits database activities, flags suspicious actions or unauthorized access attempts in real-time. DAM offers proactive insights into potential security threats, allowing swift responses and mitigation measures. By maintaining vigilant watchfulness over database interactions, DAM enhances the framework's ability to detect and counteract malicious activities promptly.

The combination of Transparent Data Encryption (TDE), data masking, redaction, and Database Activity Monitoring (DAM) within the database security subcomponent forges a resilient bastion for the data entrusted to the framework. These measures collectively uphold the sanctity of data by fortifying confidentiality, ensuring controlled access, and enabling 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

2.1.6. 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, which will be implemented and assessed later in this research. As [5] aptly noted '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 to 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 General Data Protection Regulation (GDPR) and the US Health Insurance Portability and Accountability Act (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 emulate this guidance by proposing a set of policies that will significantly influence the realization of privacy-preserving technical and semantic interoperability with robust security measures.

The following policies are implemented in the framework:

- *Compliance Monitoring Policy*: The Compliance Monitoring Policy serves as a comprehensive guide, encompassing a detailed framework of procedures, guidelines, and strategic measures. Its primary objective is to establish a robust system that ensures adherence by all stakeholders to the defined interoperability standards and regulations governing EMRs. This policy is guided by the [34] standards which advocates for consistent system monitoring.
- *Change Management Policy*: The Change Management Policy establishes the fundamental principles and procedures governing the identification, assessment, implementation, and oversight of changes within the framework. Its primary objective is to ensure a systematic and disciplined approach to change management, thereby mitigating disruptions and preserving operational efficiency within the proposed framework.
- • *Disaster Recovery and Business Continuity Policy*: The Disaster Recovery and Business Continuity Policy is an indispensable document that serves as the cornerstone of resilience .The purpose of this policy is to provide comprehensive guidance on the preservation of system data and the necessary steps and procedures to be adhered to in the event of data loss, as well as the strategies for data recovery and retrieval. This policy will encompass a thorough outline of all data recovery protocols and backup frequency specifications with the aim of minimizing data loss to the greatest extent possible.

- *Data Consent Revocation Policy*; The Data Consent Revocation Policy is a pivotal document that provides clear guidance on the process of revoking patient consent for data sharing and storage. Within this policy, the step-by-step procedures for revoking previously granted consent are meticulously defined. Moreover, it illuminates the necessary actions to be taken concerning any data that is currently stored, ensuring a transparent and accountable approach to data management. This policy serves as a safeguard for both patients and the organization, facilitating the seamless and ethical handling of sensitive healthcare data while respecting patients' rights to control their personal information. While this is implemented as part of the system during implementation, this is also documented and serves as a guide in instances where due process has not been adhered to.
- *Data Retention and Deletion Policy*: The Data Retention and Deletion Policy is a document that outlines the systematic and secure management of data within the framework. This policy outlines the crucial principles governing how data, whether sensitive or routine, is retained and eventually deleted in compliance with legal and regulatory requirements. It establishes clear guidelines for the duration of data retention, proper storage and archiving procedures, and the secure and irreversible methods for data deletion or destruction when it is no longer needed. By adhering to this policy, the responsible management of data is ensured throughout its lifecycle as well as compliance with privacy and data protection requirements.
- *Audit Logging Policy*: Is a vital document that lays out the rules and procedures for generating, storing, and monitoring audit logs of systems. These logs record crucial events and activities, serving purposes such as security monitoring, compliance verification, and troubleshooting. This policy defines what events to log, who has access to these logs, how long they should be retained, and the procedures for reviewing and protecting them. By adhering to this policy, the integrity of system audit logs are ensured, helping in the detection of security incidents, compliance with regulations, and maintaining accountability for system actions.
- *Error Handling and Reporting Policy*: This policy outlines a structured approach to classify, address, and report errors promptly and efficiently. It specifies roles and responsibilities for error resolution and escalation, emphasizing the minimization of disruptions, the preservation of data accuracy, and the enhancement of overall system reliability. Adherence to this policy, will ensure a coordinated response to errors and improve communication between the teams that are tasked with the responsibility of resolving the challenges. It also establishes a foundation for continuous improvement, learning from previous or similar errors to prevent their recurrence and bolster operational effectiveness.
- *Interoperability Testing Policy*: This policy defines the procedures and protocols for testing compatibility and seamless integration of various software, hardware, or systems. It outlines the structured approach for assessing how disparate components interact and exchange data, ensuring they function harmoniously without disruptions. This policy specifies the testing criteria, methodologies, and frequency of interoperability assessments, all aimed at verifying that diverse systems can communicate effectively. To ensure the reliability and performance of technology and infrastructure, this policy must be adhered to in order to mitigate potential issues that may arise from incompatibilities, ultimately promoting efficiency and minimizing downtime.
- *Identity and Access Management Policy*: This policy lays out the principles, procedures, and safeguards governing the access to and management of digital identities within related systems. This policy covers a wide spectrum, encompassing user authentication, authorization, role-based access controls, password management, and the safeguarding of sensitive patient data. Its primary objective is to ensure that the right individuals access the right resources, bolstering security and privacy while streamlining workflows.
- *Consent Management Policy*: This defines the procedures, guidelines, and principles for collecting, managing, and respecting individuals' consent regarding data processing and usage. This policy outlines the systematic approach to obtaining informed and explicit consent from individuals, particularly in contexts involving sensitive or personal data. It also details the procedures for maintaining consent records, providing mechanisms for individuals to withdraw their consent, and ensuring compliance with data protection laws and regulations, such as the GDPR and HIPAA.

3.0. Framework Comparison/Evaluation

The famework was evaluated by comparing it with exising (related) frameworks discussed in Section 1.2 above, based on various criteria as follows.

- Semantic Interoperability: Ensures that the meaning of exchanged data is interpreted consistently across different systems.
- Technical Interoperability: Focuses on the technical requirements for data exchange, such as communication protocols and data formats.
- Reusability: Assesses the framework's ability to be reused across different applications and contexts without significant modifications.
- Scalability: Evaluates the framework's ability to handle an increasing amount of work or its potential to be enlarged to accommodate growth.
- Compliance to Standards: Measures the extent to which the framework adheres to relevant industry standards and regulations.
- Consent Management: Looks at how well the framework manages user consent for data usage, ensuring that privacy preferences are respected.
- Access Control: Examines the mechanisms in place for restricting access to data and ensuring that only authorized users can access sensitive information.
- Network Security: Evaluates the measures taken to protect data during transmission over a network, preventing unauthorized access and data breaches.
- Identity and Access Management (IAM): Reviews the processes for managing user identities and their access to systems and data, ensuring robust authentication and authorization.
- Threat Detection and Prevention: Looks at the framework's ability to detect and prevent security threats, such as malware, hacking, and other cyber-attacks.
- Legal Interoperability: Assesses how well the framework aligns with legal requirements and supports the exchange of data across different legal jurisdictions (HIPAA and GDPR).

Table 1 compares the proposed framework against related works using the criteria discussed above.

Table 1. Framework comparism.

Criteria	eEIF	Blockchain-based	Ancile	Hyperledger-based (Access Control)	Tanzanian EHR Framework	PbDinEHR	DEPLOYR	API-led Integration	TASSIPS
Semantic Interoperability	Yes	No	No	No	Yes	Yes	No	No	Yes
Technical Interoperability	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes
Reusability	No	No	No	No	No	No	No	Yes	Yes
Scalability	Yes	No	No	No	No	No	No	Yes	Yes
Compliance to Standards	Yes	No	Yes	Yes	No	Yes	Yes	No	Yes
Consent Management	No	Yes	Yes	Yes	No	No	No	Yes	Yes
Access Control	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes
Network Security	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes
Identity and Access Management	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes
Threat Detection and Prevention	No	Yes	Yes	Yes	No	No	No	Yes	Yes
Legal Interoperability	Yes	No	Yes	Yes	No	No	No	No	Yes

Table 1 shows that the TASSIPS framework meets all the criteria assessed, and is arguably an improvement on existing interoperability frameworks for EHR/EMR.

4.0. Conclusion

The TASIPPS framework offers several distinct advantages compared to other frameworks proposed for achieving interoperability in healthcare systems. Firstly, TASIPPS takes a comprehensive approach by combining the strengths of SOA, FHIR, and SAML frameworks. This integration allows TASIPPS to address a wider range of interoperability challenges discussed in earlier chapters, including technical, semantic, privacy, and security aspects, all within a single, cohesive solution. Moreover, TASIPPS is designed with scalability and adaptability at its core, making it suitable for larger healthcare systems and nationwide adaptation and deployment. Its flexibility allows for seamless integration with existing healthcare information systems, reducing disruptions during the transition to an interoperable environment and its comparative low cost against other proposed frameworks.

Author Contributions: Conceptualization, AA., and C.G.; methodology, AA., and C.G.; validation, AA., C.G. and G.M.; formal analysis, AA., and C.G.; investigation, AA; data curation, AA.; writing—original draft preparation, AA and C.G; writing—review and editing, AA., C.G. and G.M.; visualization, AA., C.G. and G.M.; supervision, C.G; 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 was created for this article.

Acknowledgments: In this section, you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

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

References

1. Abernethy, A., Adams, L., Barrett, M., Bechtel, C., Brennan, P., Butte, A., Faulkner, J., Fontaine, E., Friedhoff, S., Halamka, J., Howell, M., Johnson, K., Long, P., McGraw, D., Miller, R., Lee, P., Perlin, J., Rucker, D., Sandy, L. and Savage, L. (2022). The Promise of Digital Health: Then, Now, and the Future. *NAM Perspectives*, 6(22).
2. Alleva (2021). EMR vs EHR: What is the Difference? | EMR vs EHR Systems. [online] Available at: https://hel-loalleva.com/emr-vs-ehr-what-is-the-difference [Accessed 3 Dec. 2021
3. Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)*, [online] pp.25–30. doi:https://doi.org/10.1109/obd.2016.11.
4. Bhartiya, S., Mehrotra, D., and Girdhar, A. (2016). Issues in Achieving Complete Interoperability while Sharing Electronic Health Records. Procedia Computer Science, 78, 192–198. doi: https://doi.org/10.1016/j.procs.2016.02.033.
5. Bincoletto, G. (2020). Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union. *Data & Policy*, 2. doi:https://doi.org/10.1017/dap.2020.2.
6. Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E. and Truscott, A. (2016). Blockchain Technology: Opportunities for Healthcare. Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. Available at: https://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf [Accessed 20 July 2024].
7. Camp, W. G. (2001). Formulating and Evaluating Theoretical Frameworks for Career and Technical Education Research. Journal of Vocational Educational Research, 26 (1), 27-39.
8. Christodoulakis, C., Asgarian, A. and Easterbrook, S. (2017). November. Barriers to adoption of information technology in healthcare. In *Proceedings of the 27th Annual International Conference on Computer Science and Software Engineering* (pp. 66-75).
9. Corbin, C.K., Maclay, R., Acharya, A., Mony, S., Soumya Punnathanam, Thapa, R., Kotecha, N., Shah, N.H. and Chen, J. (2023). DEPLOYR: a technical framework for deploying custom real-time machine learning models into the electronic medical record. *Journal of the American Medical Informatics Association*. doi:https://doi.org/10.1093/jamia/ocad114.
10. Dagher, G.G., Mohler, J., Milojkovic, M. and Marella, P.B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, 39, pp.283–297. doi:https://doi.org/10.1016/j.scs.2018.02.014.
11. Eder, E., Wiegand, M., Krieg-Holz, U., and Hahn, U. (2022). "beste grüße, maria meyer" — pseudonymization of privacy-sensitive information in emails. In Proceedings of the Thirteenth Language Resources and Evaluation Conference, pages 741–752, Marseille, France. European Language Resources Association.

12. Ertmer, P. A., and Newby, T. J. (2013). Behaviorism, cognitivism, constructivism: Comparing critical features from an instructional design perspective. Performance Improvement Quarterly, 26(2), 43-71.
13. Ganck, A.D. (2017). *The New European Interoperability Framework*. [online] ISA^2 - European Commission. Available at: https://ec.europa.eu/isa2/eif_en/.
14. García-Closas, M., Ahearn, T.U., Gaudet, M.M., Hurson, A.N., Balasubramanian, J.B., Choudhury, P.P., Gerlanc, N.M., Patel, B., Russ, D., Abubakar, M. and Freedman, N.D. (2023). Moving toward findable, accessible, interoperable, reusable practices in epidemiologic research. *American journal of epidemiology*, *192*(6), pp.995-1005.
15. GDPR (2018). *Article 5 📖 GDPR. Principles relating to processing of personal data | GDPR-Text.com*. [online] Available at: https://gdpr-text.com/read/article-5/.
16. Grant, C. and Osanloo, A. (2014). Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blue print f or 'House'. Administrative Issues Journal: Connecting Education, Practice and Research, Pp. 12-22 DOI: 10.5929/2014.4.2.9
17. IBM (2023). What is a REST API? | IBM. [online] www.ibm.com. Available at: https://www.ibm.com/topics/rest-apis.
18. IEEE (2013). Standards glossary, Retrieved from http://www.ieee.org/education_careers/education/standards/standards_glossary.html.
19. ISO (2020). *ISO/TR 20514:2005*. [online] ISO. Available at: https://www.iso.org/standard/39525.html.
20. Ivan D. **(2016).** Moving toward a blockchain-based method for the secure storage of patient records. In: ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, MD, United States: ONC/NIST, August 2016; 2016, pp. 1–11.
21. Itirra. (2023). *What is HL7? Advantages and Disadvantages Explained | Blog*. [online] Available at: https://itirra.com/blog/hl7advantagesdisadvantages/#:~:text=What%20are%20the%20disadvantages%20of%20HL7%3F&text=HL7%20standards%20can%20be%20complex [Accessed 24 Jun. 2023].
22. Kouroubali, A. and Katehakis, D.G. (2019). The new European interoperability framework as a facilitator of digital transformation for citizen empowerment. *Journal of Biomedical Informatics*, 94, p.103166. doi:https://doi.org/10.1016/j.jbi.2019.103166.
23. Kunshu ,W. , Xiangjun Wu, H. W., Haibin K. , and Jurgen, K. (2021). New color image cryptosystem via SHA-512 and hybrid domain, Multimed. Tools Appl. 80(12) (2021) 18875–18899.
24. Liehr, P. and Smith, M.J. (1999). Middle Range Theory: Spinning Research and Practice to Create Knowledge for the New Millennium. *Advances in Nursing Science*, 21(4), pp.81–91. doi:https://doi.org/10.1097/00012272-199906000-00011.
25. Lin, Q., Wang, H., Pei, X. and Wang, J. (2019). Food Safety Traceability System Based on Blockchain and EPCIS. *IEEE Access*, 7, pp.20698–20707. doi:https://doi.org/10.1109/access.2019.2897792.
26. Linn, L.A. and Koo, M.B. (2016). 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. Available at: https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf [Accessed 20 July 2024]
27. López, D.M.,González, C., and Blobel, B., (2010). Ontology-based interoperability service for HL7 interfaces implementation. In *Seamless Care–Safe Care* (pp. 108-114). IOS Press.
28. Luse, A., Mennecke, B. and Townsend, A. (2012). Selecting a Research Topic: A Framework for Doctoral Students. *International Journal of Doctoral Studies*, 7, pp.143–152. doi:https://doi.org/10.28945/1572.
29. Merriam, S. B., and Tisdell, E. J. (2015). Qualitative research: A guide to design and implementation (4th ed.). John Wiley & Sons.
30. Miles, M. B., and Huberman, A. M. (1994). Qualitative Data Analysis An Expanded Sourcebook. Thousand Oaks, CA Sage Publications. - References - Scientific Research Publishing. [online] Available at: https://www.scirp.org/reference/referencespapers?referenceid=1423956.
31. Mishra, R., Kaur, I., Sahu, S., Saxena, S., Malsa, N. and Narwaria, M. (2023). Establishing three layer architecture to improve interoperability in Medicare using smart and strategic API led integration. SoftwareX, [online] 22, p.101376. doi:https://doi.org/10.1016/j.softx.2023.101376.
32. Mwogosi, A. (2023). Digital Transformation in Tanzania's Healthcare Sector: A Systematic Review of Robust Electronic Health RecordsSystems' Critical Success Factors. *Research Square (Research Square)*. doi:https://doi.org/10.21203/rs.3.rs-3034281/v1.
33. Ntafi, C., Spyrou, S., Bamidis, P. and Theodorou, M. (2022). The legal aspect of interoperability of cross border electronic health services: A study of the european and national legal framework. *Health Informatics Journal*, 28(3), p.146045822211287. doi:https://doi.org/10.1177/14604582221128722.
34. Oracle.com. (2023). *Risk and Compliance*. [online] Available at: https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/risk-and-compliance.htm.

35. Palma, F., Olsson, T., Wingkvist, A. and Gonzalez-Huerta, J. (2022). Assessing the linguistic quality of REST APIs for IoT applications. Journal of Systems and Software, 191, p.111369. doi:https://doi.org/10.1016/j.jss.2022.111369.
36. Peterson, K.J., Deeduvanu, R., Kanjamala, P. and Mayo, K. (2016). A Blockchain-Based Approach to Health Information Exchange Networks. [online] www.semanticscholar.org. Available at: https://www.semanticscholar.org/paper/A-Blockchain-Based-Approach-to-Health-Information-Peterson-Deeduvanu/c1b189c81b6fda71a471adec11cfe72f6067c1ad.
37. Pierre, L., Ildikó P., David, S. , Montserrat B. and Lilja, Ø. **(**2021**)**. 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), pages 4188–4203, Online. Association for Computational Linguistics.
38. Pilán, I., Lison, P., Øvrelid, L., Papadopoulou, A., Sánchez, D. and Batet, M. (2022). The Text Anonymization Benchmark (TAB): A Dedicated Corpus and Evaluation Framework for Text Anonymization. *Computational Linguistics*, 48(4), pp.1053–1101. doi:https://doi.org/10.1162/coli_a_00458.
39. Rajput, A. R., Li, Q. and Ahvanooey, M. T. **(2021).** "A blockchain-based secret-data sharing framework for personal health records in emergency condition", Healthcare, vol. 9, no. 2, pp. 206, Feb. 2021.
40. Reis, Z.S.N., Maia, T.A., Marcolino, M.S., Becerra-Posada, F., Novillo-Ortiz, D. and Ribeiro, A.L.P. (2017). Is There Evidence of Cost Benefits of Electronic Medical Records, Standards, or Interoperability in Hospital Information Systems? Overview of Systematic Reviews. *JMIR Medical Informatics*, 5(3), p.e26. doi:https://doi.org/10.2196/medinform.7400.
41. Ross, G.M.S., Zhao, Y., Bosman, A.J., Geballa-Koukoula, A., Zhou, H., Elliott, C.T.,. Nielen, M.W.F. ., Rafferty, K., and Salentijn, G.IJ. (2023) .Best practices and current implementation of emerging smartphonebased (bio)sensors - Part 1: Data handling and ethics,TrAC Trends in Analytical Chemistry, 158 doi: https://doi.org/10.1016/j.trac.2022.116863.
42. Selvapriya, E.S. and Suganthi, L. (2023). Design and implementation of low power Advanced Encryption Standard cryptocore utilizing dynamic pipelined asynchronous model. Integration, [online] 93, p.102057. doi:https://doi.org/10.1016/j.vlsi.2023.102057.
43. Semantha, F.H., Azam, S., Shanmugam, B. and Yeo, K.C. (2023). PbDinEHR: A Novel Privacy by Design Developed Framework Using Distributed Data Storage and Sharing for Secure and Scalable Electronic Health Records Management. *Journal of Sensor and Actuator Networks*, [online] 12(2), p.36. doi:https://doi.org/10.3390/jsan12020036.
44. Sharma, P., Borah, M.D. and Namasudra, S. (2021). Improving security of medical big data by using Blockchain technology. Computers & Electrical Engineering, 96, p.107529.
45. Shinozaki, A. (2020). Electronic Medical Records and Machine Learning in Approaches to Drug Development. [20 July 2024]
46. Singh, J. and Chaudhary, N.K. (2022). OAuth 2.0: Architectural design augmentation for mitigation of common security vulnerabilities. Journal of Information Security and Applications, 65, p.103091. doi:https://doi.org/10.1016/j.jisa.2021.103091.
47. Singh, S. (2023). What is a Conceptual Framework and How to Make It (with Examples). Researcher.Life. Available at: https://researcher.life/blog/article/what-is-a-conceptual-framework-and-how-to-make-it-with-examples/.
48. Spanakis, E.G., Sfakianakis, S., Bonomi, S., Ciccotelli, C., Magalini, S. and Sakkalis, V. (2021). Emerging and Established Trends to Support Secure Health Information Exchange. *Frontiers in Digital Health*, 3. doi:https://doi.org/10.3389/fdgth.2021.636082.
49. Van Der Veer, H. and Wiles, A. (2008). Achieving Technical Interoperability - the ETSI Approach. [online]
50. WHO (2024). *Digital Health and Innovation*. [online] Available at: https://www.who.int/publications/m/item/digital-health-and-innovation [Accessed 20 Jul. 2024]
51. Yan, X., Wu, Q., and Sun, Y. (2020). A Homomorphic Encryption and Privacy Protection Method Based on Blockchain and Edge Computing. Wireless Communications and Mobile Computing, 2020, Article ID 8832341. https://doi.org/10.1155/2020/8832341
52. Yang, H., and Yang, B. (2017). A Blockchain-Based Approach to the Secure Sharing of Healthcare Data. In Proceedings of the Norwegian Information Security Conference 2017 (pp. 100–111). NIKS.
53. Young, P., Chaki, N., Berzins, V., and Luqi, L. (2003). Evaluation of middleware architectures in achieving system interoperability, Rapid Systems Prototyping Proceedings, 14th IEEE International Workshop, pp. 108-116.

54. Yuan, H., Wang, Z., Chen, Z., Gong, Y., Lu, J., Hu, Y., Li, L. and Qian, F. (2023). A Fine-Grained Access Control Method Based on Role Permission Management. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICDCECE57866.2023.10150760.
55. Yue, Z., Ding, S., Zhao, L., Zhang, Y., Cao, Z., Tanveer, M., Jolfaei, A. and Zheng, X. (2021). Privacy-preserving time-series medical images analysis using a hybrid deep learning framework. *ACM Transactions on Internet Technology (TOIT)*, *21*(3), pp.1-21.

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.