Building an Interoperable, Open, and Patient-Centric Global Architecture for Personal Health Data Management

Ricardo Ribeiro, Aneesh Zutshi and António Grilo

July 11, 2023

Building an Interoperable, Open, and Patient-Centric Global Architecture for Personal Health Data Management: Literature Review and Proposed Architecture

Ricardo Ribeiro [a.], Aneesh Zutshi [a, b, c], Antonio Grilo [a, b, c]

a. Department of Industrial Engineering and Management at NOVA University Lisbon, Portugal; Campus FCT/UNL - 2829-516 Caparica;

b. UNIDEMI, Department of Mechanical and Industrial Engineering, NOVA School of Science and Technology, Universidade NOVA de Lisboa, 2829-516 Caparica, Portugal

c. Laboratório Associado de Sistemas Inteligentes, LASI, 4800-058 Guimarães, Portugal

Abstract

This paper presents a comprehensive analysis of the need for a global architecture for personal health data management that is interoperable, open, and patient-centric. The healthcare industry is ripe for disruption with the rapid advancement of digital technologies and the increasing patient demand for control over their data. This paper explores the challenges and opportunities in building such an architecture and proposes research questions to address critical elements, including interoperability, applications, and incentivising private players. The literature review delves into various topics such as data management, standards, interoperability, patient data ownership, identity management, and user-centric design in health data systems. The role of health information exchanges and the adoption of standards are also discussed. Drawing inspiration from other industries, such as banking, telecommunications, government, smart home, energy and utilities, transportation, and mobility, this paper highlights the benefits and challenges of implementing open standards and interoperability. It emphasises the importance of adopting a patient-centric, interoperable, and open architecture for healthcare data management, outlining fundamental principles and proposing a multi-layered architecture design. This architecture aims to address the evolving needs of healthcare data management, focusing on interoperability, patient-centricity, and openness while ensuring privacy, security, and governance. The next step in this research is to validate the proposed architecture in the market and refine it based on real-world feedback and performance. By doing so, we can ensure that the architecture meets the needs of all stakeholders involved in healthcare data management. Ultimately, this research aims to contribute to developing an interoperable, open, and patient-centric global architecture for personal health data management, revolutionising the healthcare industry and empowering patients to take control of their health data.

Keywords: Personal Health Data Management; Interoperability; Patient-Centric; Open Architecture; Healthcare Industry Disruption

1. Introduction

The healthcare industry has the most impact on human life and well-being and, consequently, is the industry to which most human capital gets devoted. The rapid evolution of digital technologies, the increased patient demand to actively participate in their health journey, and their willingness to have more control over their data create the perfect scenario for disruption.

In this new World that some authors call Healthcare 3.0 [1], new ways to provide Healthcare will emerge based on the innovation of bright minds leveraged by the technological acceleration we already see

today, focused on human well-being and longevity. Soon, it will be possible to integrate and combine data, from medical records to personal health records, including lifestyle information which drives an accurate, holistic view of private and public health. High levels of interoperability between health information systems will be achieved securely, and the patient will be in control of their data and consequently have a leading role in the healthcare journey in their life. Holistic data combined with machine learning systems could identify patterns to improve deep analytical abilities about developing health conditions, suggest preventive practices, and even advise consultations, second opinions and interventions, from general practice to precision medicine. The combination of the Internet of Things and faster data transfer will enable remote Healthcare not only for developed regions but primarily for unserved populations around the World. The broader use of blockchain to secure data transactions and distributed storage will give rise to new ways of putting people in control of its information. Every journey is digital in this new World. Therefore, every person must have a unique digital identity representation, which will act differently according to the context and need by designing personas based on concepts such as Self-Sovereign Identity.

However, today's healthcare ecosystem has yet to be at this stage. The existing healthcare data management systems are siloed and fragmented. This fragmentation leads to a need for a unified patient health record, conducting patient identification and matching difficulties. Moreover, it can also create problems in data retrieval, usually resulting in inadequate or delayed care. Even though various interoperability standards have been introduced, such as Health Level Seven (HL7), Fast Healthcare Interoperability Resources (FHIR), and Digital Imaging and Communications in Medicine (DICOM), they need more success to ensure seamless integration of health data.

Data's volume, velocity, and structured and unstructured nature present unique challenges. The exponential growth of medical data, which includes electronic health records (EHR), imaging data, genetic information, wearable device data, and other health-related information, has overtaken the ability of existing systems to manage and analyse it effectively. This fact has led to inefficient use of this valuable resource.

Data privacy and security are another critical concern. Healthcare data is a significant target for cyber-attacks due to its value. Despite rigorous regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), breaches exposing sensitive patient information continue to occur. For example, in 2020, more than 28 million records were exposed, compromised, or impermissibly disclosed [2].

Furthermore, although broadly accepted as the way forward, the patient-centric model faces implementation challenges. For patients to take ownership of their health data and participate actively in their care, they need access to their health records, understand them, and make informed decisions based on this information. [3]

The lack of universally accepted and implemented unique digital identities presents another challenge. Although the promise of Self-Sovereign Identity, its application is still a work in progress, with many technical, legal, and societal obstacles to overcome.

Lastly, the cost of transitioning to a more integrated, interoperable, and patient-centric system can be very high, primarily for smaller health service providers. It requires significant monetary investment and imposes a change in practices, workflows, and mindset among all stakeholders, including physicians and patients.

In conclusion, building an interoperable, open, and patient-centric global architecture for personal health data management is a complex endeavour with many challenges. However, it also creates significant opportunities for innovation and development.

2. Research Questions

The following research questions address several topics related to designing and implementing an open health data architecture. The first question identifies the critical elements of such an architecture, including data interoperability, standards, data storage options, identity management, permission access, and data ownership. The second question explores how an open data architecture can promote interoperability in healthcare information exchange and encourage the participation of service providers through principles like open-source development, open protocols, and accessible APIs. The third question investigates the potential applications and business models that can emerge with the referred architecture, ranging from remote medical assistance and precision medicine innovations to Ai-assisted diagnosis and dynamic insurance pricing schemes. Finally, the fourth question delves into the structure needed to incentivise private players to contribute to this infrastructure, considering aspects such as governance, data privacy, internal policies, and competition to build new products and services that meet the emergent demand of patients and other healthcare stakeholders.

RQ1: What are the critical elements of an open data health architecture?

RQ2: How can an open data architecture be designed to promote interoperability in healthcare information exchange and encourage open participation from service providers?

RQ3: What applications and business models can emerge within an open health data architecture?

RQ4: What would be the structure to incentivise the private players to build up on this infrastructure?

3. State of the Art

An in-depth literature review will be conducted to address the research questions, and the main topics are presented below. For each main topic, the relevant literature review will be explored to understand existing knowledge and identify gaps to where this investigation may contribute.

3.1 The Landscape of Data, Standards, and Interoperability in Healthcare Data Management

Health Data

In the modern healthcare landscape, the role of data has become increasingly paramount. The exponential growth of data sources has led to a surge in health data volume and variety [4], with the Medical Internet of Things (MioT) adding another layer of complexity. Health data encompasses a wide range of information, from clinical records and imaging results to pharmaceutical data and patient-reported outcomes. It also includes data sourced from wearable devices, social determinants of health, patient demographics, and billing or insurance information [5].

In the digital age, most of this data is unstructured, which, while rich in insights, poses challenges due to the need for uniformity in format and structure. For instance, structured data includes patient demographics, billing, insurance, pharmaceutical, laboratory, genomic, wearable device data, International Classification of Diseases (ICD), and Social Determinants of Health (SDOH) [6]. In contrast, unstructured data includes clinical notes, email correspondence with patients, accessible text in Electronic Health Records (HER), medical imaging, transcripts of voice recordings, patient letters, physician's handwritten notes, and narrative patient histories.

Health Data Systems

To manage, exchange, and effectively use this patient information, several data systems converge. These include Electronic Health Records (HERs), Health Information Exchanges (HIEs), Personal Health

Records (PHRs), and Practice Management Systems (PMS). Each system plays a specific role, complementing each other to create a seamless health information network.

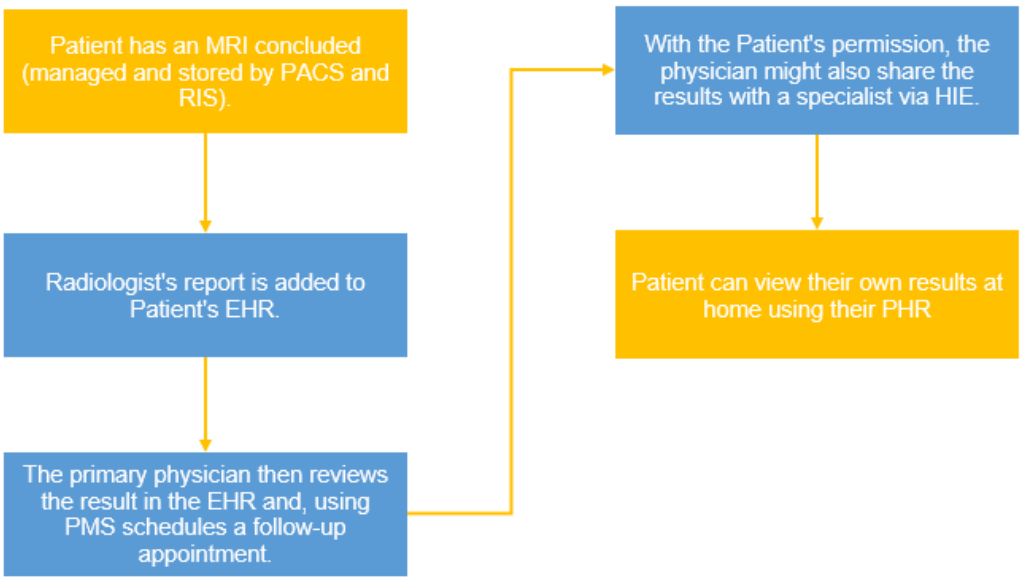

Figure 1 - Example of how Data Systems work based on a specific patient case.

Electronic Health Records (HERs) contain a comprehensive record of a patient's medical history, diagnosis, medications, treatment plans, immunisation dates, allergies, imaging, laboratory, and test results. Health Information Exchanges (HIEs) allow patients and healthcare professionals to access and securely share patient medical information. HIEs can be categorised into three types: directed exchange for sending and receiving information between healthcare providers; query-based for providers to find and or request information from other providers; and consumer-mediated for patients to aggregate and control the use of their information among providers.

Personal Health Records (PHRs) are health records (data) under the patient's control, usually in digital format. They can be stored in patients' devices or pulled from connected EHR systems. Practice Management Systems (PMS) support the daily operations of healthcare providers, such as scheduling appointments, billing, reporting, and managing patient data. Other systems, such as Picture Archiving and Communication Systems (PACS), provide storage and access to images from multiple types and origins. These systems typically work with the Radiology Information Systems (RIS). Other systems, such as Laboratory Information Systems (LIS), which manage and store data from laboratory results, and Pharmacy Information Systems, are designed to meet the needs of the pharmacy's internal department.

Interoperability in Health Information Systems is a critical aspect of this landscape. The International Standard Organisation (ISO) defines the interoperability of Electronic Health Records (EHRs) as "the ability of two or more applications being able to communicate effectively without compromising the content transmitted" [7]. For the Health Information and Management Systems Society (HIMSS), interoperability is "the ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged" [8]. Both definitions highlight the importance of transmitting data and ensuring the content remains intact and usable after the exchange, effectively capturing the essence of interoperability in Healthcare.

Standards and Interoperability

One of the essential aspects of achieving interoperability is the universal adoption of standards, such as Health Level Seven (HL7), Digital Imaging and Communications in Medicine (DICOM), and Fast Healthcare Interoperability Resources (FHIR). These standards provide a framework for consistently transmitting, exchanging, and retrieving electronic health information, enabling various systems to understand the same data elements in the same way.

According to the HIMSS internet page [9], over 40 Standards Development Organisations (SDOs) exist in the health information technology landscape. These organisations are responsible for the standards life cycle, from producing to promulgating, even emending, and interpreting them. Entities such as the American National Standards Institute (ANSI) or the International Organisation for Standardisation (ISO) accredit these SDOs.

However, the adoption of these standards is not without challenges. The considerable fragmentation of standards due to their variety and specific focus areas can lead to cases where data exchange is possible only between systems that have implemented the same standards. Moreover, proprietary standards can potentially lead to a monopolistic situation where healthcare providers are locked into a particular technology or vendor, making transitioning to different systems or technologies costly and challenging.

Developing new open standards like OpenEHR is an excellent opportunity to mitigate this scenario. OpenEHR is an open-source standard developed by OpenEHR Foundation, a non-profit organisation for implementing electronic health record systems. It provides a framework for creating interoperability, vendor-neutral HER systems that can be customised to meet the specific needs of healthcare providers.

Significant challenges still exist despite the benefits of applying OpenEHR standards and architecture. According to Ulriksen [10], coordinating users from different healthcare levels is one of these. Creating new archetypes from scratch or modifying existing ones to meet specific requirements is a substantial endeavour. Developing and agreeing on archetypes nationally (and internationally) becomes difficult due to the users' varied backgrounds, knowledge levels, perspectives, and negotiation powers. Moreover, archetypes are generally agreed upon and defined before being tested or implemented in clinical settings, indicating a potential disconnect between theoretical standards and practical day-to-day operations. As projects scale up, complex socio-technical issues may arise that can be neglected in smaller pilot projects. In conclusion, the mentioned challenges underline the complexity of adopting a flexible, user-centred approach to standardisation, such as OpenEHR, mainly when implemented on a large scale [10]

Terminologies, vocabularies, and ontologies

Another critical aspect of the healthcare data landscape is the set of common terminologies, vocabularies, and ontologies [11], as they are integral in how data and information is structured, understood, and shared across various health systems.

Terminologies refer to sets of terms representing a system of concepts, such as the International Classification of Diseases (ICD), that provides a standardised system for classifying diseases and other health issues. Vocabulary is a standardised set of words or phrases that provides the codes used to represent clinical concepts, ensuring consistency across different systems. Ontologies organise information and knowledge into a hierarchy of concepts and relationships. Its role formally defines categories, properties, and relations between concepts, data, and entities across domains.

The Role and Adoption of Health Information Exchanges

As a technology-driven process, Health Information Exchanges (HIEs) facilitate interoperability in the healthcare ecosystem by enabling data exchange among healthcare providers, such as hospitals, clinics, pharmacies, and laboratories. By doing this, health information exchanges ensure that all providers involved in a patient's care have access to the same information. They are also responsible for supporting

the use of standards such as the ones mentioned above to ensure that data can be seamlessly shared and understood across different health systems, therefore speaking the same language. They also play an essential role in safeguarding that the data exchange complies with privacy and security standards and regulations, such as HIPAA and GDPR, which are critical for preserving trust between all stakeholders.

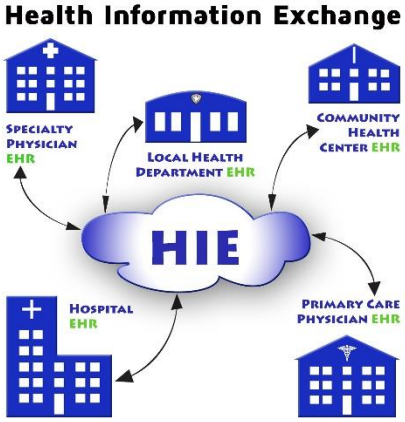

Figure 2 - Health Information Exchange Diagram. Retrieved from https://patagoniahealth.com/blog/what-is-health-information-exchange-and-why-is-it-important-for-ehr-use/ at 30/05/2023.

Adopting Health Information Exchange (HIE) and ensuring interoperability is a significant milestone for improving patient care. However, these advancements are not without challenges, as identified in recent studies [12][8]. In exploring the barriers to HIE adoption, Dixon et al. [12] identified that perceptions of HIE's benefits and risks, specifically those associated with trust, privacy, data accuracy, and potential misuse of information, significantly influence its acceptance among healthcare professionals. Concerns over the possible misuse of patient data, privacy breaches, and inaccurate data interpretations can impede the complete utilisation of HIE. To promote trust and facilitate IEH adoption, the author recommends robust regulatory frameworks and effective measures to satisfy these concerns [12].

Torab-Miandoab et al. [8] systematic literature review emphasises barriers such as ambiguous standards prone to local interpretation, resistance to transitioning from paper-based to electronic systems, and outdated systems with limited interoperability capabilities. Furthermore, the authors found that concerns about privacy and security linked with a lack of administrative and legal support for changes in Information Technology (IT) practices equally pose significant challenges to interoperability. The Legacy systems are also an effective barrier identified. These systems were initially developed for specific activities, and many were designed to limit compatibility with other applications to protect market share, thereby hindering interoperability. Resistance to change presents another critical challenge [8]. This resistance often arises from healthcare professionals' hesitation about adopting new technology and the perceived burden of learning new systems. Other barriers include inadequate funding for IT resources and a need for uniform systems from different vendors.

3.2 The complexities of patient data ownership, data control, and privacy within the healthcare system.

Patient data ownership, data control, and the privacy landscape in the healthcare system are complex and multifaceted. This complexity arises from the legal and ethical implications of patient data ownership, the existing frameworks for data ownership and access controls, the impact of data breaches in Healthcare, and the privacy laws and regulations affecting how data is collected, shared, and used.

Understanding the concept of patient data ownership is crucial. Data ownership, particularly in Healthcare, has substantial implications for biomedical research, individual freedom, and the free-market economy [13]. Despite rigorous regulations, primarily in developed countries, the inherent

complexity of the subject continues to feed ongoing debates. Two prominent perspectives dominate these discussions: proponents of private ownership, who view it as a path for individual control over their data, privacy, and property, and advocates of public ownership, who perceive individual-level health data as a shared resource or a common good [13].

The importance of data ownership becomes even more evident when examining the potential ramifications of limited access and control over personal health data. According to Kish and Topol's "Unpatients – why patients should own their medical data" [3], the lack of immediate access to health information contributes to an estimated 20% of preventable medical errors. These errors, in turn, result in an estimated 80,000 deaths out of the approximately 400,000 preventable medical error-related fatalities in the United States each year. The statistic reveals that in 49 out of 50 states in the United States, the ownership of medical records is predominately entrusted to physicians and hospitals, not patients. This ownership paradigm is embedded in paternalism by the medical community's conviction that patients might not be equipped to manage or use their data. However, evidence suggests otherwise, indicating that patients can own and manage their data [3]. This empowerment improves their well-being and encourages the doctor-patient relationship, thus emphasising the critical nature of data ownership in the healthcare industry.

Data privacy laws and regulations significantly influence health data ownership across various geographies. Each region has implemented unique legal frameworks to balance patient privacy, individual rights, and broader societal interests, impacting the healthcare industry. These laws and regulations include the Data Protection Act 2018 in the United Kingdom, the General Data Protection Regulation (GDPR) in the European Union, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the Privacy Act 1988 and the Australian Privacy Principles (APPs) in Australia, the Protection of Personal Information Act (POPIA) in South Africa, the Personal Information Protection Law (PIPL) in China, the Personal Data Protection Act 2012 (PDPA) in Singapore, and the Digital Personal Data Protection Bill 2022 in India.

Despite the varying degrees of patient control over their health data, a consistent argument across these regulations is the importance of consent and transparency. As we move forward to an exponentially data-driven world, the nuances of these laws and the equilibrium between stakeholders' competing interests will continue to model the landscape of health data ownership and use.

Data breaches in Healthcare pose a significant threat to patient data privacy. According to the paper "Healthcare Data Breaches: Insights and Implications" [14], the healthcare sector has faced the highest number of data breaches. From 2005 to 2019, the total number of individuals affected by healthcare data breaches was 249.09 million. Of these, 157.40 million individuals were affected in the last five years alone. The healthcare industry is particularly vulnerable to hacking attacks, with a significant increase in health records exposed through this form from 2005 to 2019. Other less prevalent causes include physical damage attacks, portable device management attacks, and stationary computer loss attacks, all of which have decreased in frequency in the most recent five-year period.

The implications of these breaches are severe for healthcare providers and patients. The financial, operational, and reputational risks are significant for healthcare providers. Over the five years from 2014 to 2019, the overall average cost of data breaches increased by 12%, and each breach record's cost saw a 3.4% rise [14]. This growth rate was even more prominent in the healthcare industry, where the cost per breached record rose by 19.4%, suggesting a distinct vulnerability [14].

For patients, the implications are also very significant. Privacy violations can lead to the theft of all the sensitive information collected by healthcare providers from patients during a data breach. This information includes the patient's full name, address history, financial information, and social security number, among other susceptible data. The stolen records can be sold on the dark web for up to $1000,

and people can use them to create false identities, perform illegal activities, buy illicit drugs, or even claim false insurance [15]

In conclusion, data breaches in the healthcare industry reveal a concerning scenario, showcasing high intrusion rates, affecting many patients, and increasing cost per breach, even compared with other highly regulated industries, such as financial services.

3.3 Identity Management and Self-Sovereign Identity in Healthcare.

The concept of Identity is multifaceted, extending far beyond our initial perceptions. Windley [16]states, "Identity is bigger and more complicated than you think." Identity can take on various forms, from human identities rooted in tangible attributes like fingerprints and DNA to intangible ones such as personal beliefs and experiences. The digital age has further expanded this concept, introducing machine identities represented by unique identifiers like MAC addresses, GUIDs, or VINs. In digital Identity, Windley put forward that we do not possess a single identity but rather multiple "personas" that shift according to each Identity use case [16].

Identity management is crucial across various industries, particularly in Healthcare. Misidentification can lead to harmful consequences, such as incorrect medication prescribing, invasive procedures performed on the wrong patient, or distressing diagnostic results delivered to the wrong individual. These errors harm the patients involved and undermine trust in the healthcare system.

The healthcare ecosystem, encompassing primary healthcare providers, clinical laboratories, pharmaceutical companies, and health insurance companies, interacts with identity data in several ways. Each entity is responsible for ensuring data accuracy, privacy, and security, complying with related laws and regulations. Identity data is collected and managed in various ways across these entities. For instance, healthcare providers collect identity data during patient interactions, typically recording and managing this data in Electronic Health Records (EHRs). Clinical laboratories and pharmaceutical companies also collect and manage identity data, often anonymising or de-identifying data to protect identities while tracking individual treatment responses over time. Health insurance companies collect and manage identity-related data for various activities during the health policy lifecycle.

However, managing Identity in Healthcare presents several challenges [17]. Each healthcare provider uses different patient identifiers, challenging a consolidated view of patient services. Identity data inconsistencies often arise due to nicknames, hyphenated names, last name changes, last name reversal, and frequent address and phone number changes. These inconsistencies complicate the process of patient identification matching, leading to duplication of services, assessments, and test results. This situation increases the cost of care delivery to patients and healthcare providers, underscoring the need to develop and implement globally accepted identity management systems and protocols that enable successful Identity matching [18].

Several techniques and approaches are used worldwide for patient Identity matching [19], including Unique Patient Identifiers (UPIs), algorithmic techniques, referential matching software, biometric identification systems, Radio Frequency Identification (RFID), and hybrid models. Each technique has advantages and disadvantages, which must be considered when implementing them.

The management of digital identities is facilitated by frameworks known as Identity Management Architectures (IMAs) [20]. These architectures can be categorised into four types: Independent, Centralised, Federated, and Decentralised. The Decentralised Identity Management Architecture, powered by blockchain technology, offers a promising solution for self-sovereign identity management, enhancing privacy, security, and user control.

Self-Sovereign Identity (SSI) is the next evolution of identity management models. It allows identity holders to have better control over their identity data, with a strong emphasis on data portability and data minimisation. This model addresses the deficiencies of traditional digital identity management architecture, which heavily relies on centralised data repositories and identity providers.

SSI is characterised by ten principles that differentiate it from the centralised identity management architectures. These principles include existence, persistence, control, access, transparency, portability, interoperability, consent, minimisation, and protection. Each principle offers a unique advantage over traditional Centralised IMAs.

Decentralised Identity uses cryptography, digital wallets, and related technologies to enable multiple entities to contribute credentials and empower individuals to manage their data. Decentralised Identity Systems create a trust triangle that links issuers, holders, and verifiers. These roles and information flow form the basis for this specification, with each role performed by different entities in a decentralised identity ecosystem where verifiable credentials are expected to be helpful.

Holders, for instance, possess one or more verifiable credentials and generate verifiable presentations from them. These could be students, employees, or customers. On the other hand, issuers assert claims about one or more subjects, create a verifiable credential from these claims, and transmit the verifiable credential to a holder. Corporations, non-profit organisations, trade associations, governments, and individuals can all be issuers. Subjects are entities about which claims are made, such as human beings, animals, and things. In many cases, the holder of a verifiable credential is the subject, but in some instances, it is not. For example, a parent (the holder) might hold the verifiable credential of a child (the subject).

Verifiers receive one or more verifiable credentials, optionally inside a verifiable presentation, for processing. These could be employers, security personnel, and websites. Verifiable Data Registries mediate the creation and verification of identifiers, keys, and other relevant data, such as verifiable credentials schemas, revocation registries, and issuer public keys, which might be required to use verifiable credentials. Some configurations require correlated identifiers for subjects. Examples may include trusted databases, decentralised databases, government ID databases, and distributed ledgers. Often there is more than one type of verifiable data registry used in an ecosystem.

In conclusion, identity management and self-sovereign Identity in Healthcare are complex but crucial processes. As the digital World continues to evolve, adopting and maturing these techniques and approaches will play a central role in successfully managing digital identities in Healthcare.

3.4 Application of interoperability and open standards across different industries.

This section delves into how various industries have tackled interoperability issues between systems, the lessons that can be learned from these practices, and emerging trends concerning interoperability and open standards.

Open Banking

Open Banking, a transformative initiative in the financial sector, has redefined how banks operate and interact with third-party entities. This system, which mandates banks to share their data via Application Programming Interfaces (APIs) with third parties, has its roots in the 1980s. The evolution of Open Banking has been marked by significant milestones, such as the introduction of the Home Banking Computer Interface (HBCI) in 1989, the replacement of HBCI by Financial Transaction Services (FinTs) in 2002, and the implementation of the second Payment Services Directive (PSD2) in 2007. The PSD2 has been instrumental in promoting an integrated and efficient European payments market,

fostering competition and innovation among payment service providers, especially emerging fintech startups [21].

The United Kingdom has been a frontrunner in the Open Banking movement. In 2016, the Competition and Markets Authority (CMA) mandated the nine largest banks to provide licenced startups with direct access at the transaction level. This movement responded to the lack of competition in the UK banking industry and has since set a precedent for other countries. India, Australia, and Singapore have followed suit, each adopting unique approaches to Open Banking. For instance, the Reserve Bank of India (RBI) established the Unified Payments Interface (UPI) [22], a real-time payment system that fosters financial inclusion and enables fintech innovation.

The driving forces behind Open Banking include technological advancements, changing consumer expectations, and regulatory push. Consumers today expect seamless experiences from banks, similar to other digital platforms. They want control over their financial data and the ability to share it with trusted third parties in exchange for value-added products and services. Regulatory bodies have also played a crucial role in promoting Open Banking, with the European Commission currently working on a revised version of the PSD2, known as the PSD3.

Other Industries

Several other industries have embraced Open standards and interoperability, leading to transformative changes. In the telecommunications industry, the advent of Voice over IP (VoIP) and Internet Protocol (IP)-based networks has led to the adoption of open standards like the Session Initiation Protocol (SIP).

Government open data initiatives worldwide have increased transparency, fostered innovation, and empowered citizens. These initiatives make a wide range of public data available, allowing researchers, developers, and businesses to build applications and services based on open data.

The smart home industry and the Internet of Things (IoT) have worked towards interoperability and open standards to ensure seamless integration and data exchange among various smart devices. Similarly, the energy and utilities sector has adopted open standards and interoperability to enable smart grids and metering systems, helping consumers monitor their energy usage and optimising consumption.

Open platforms and standards for sharing data among various stakeholders have risen in the transportation and mobility industry. For example, the General Transit Feed Specification (GTFS) is an open format for public transportation schedules and geographic data, enabling developers to create applications that provide route planning, real-time updates, and multimodal journey information.

In conclusion, Open Banking and other industries have embraced the application of open standards, and interoperability provides valuable insights for the healthcare sector. By adopting an open health-data management system, healthcare providers can facilitate improved patient care and mitigate the monopolistic consequences caused by centralised health data storage. This enables a gradual shift towards more significant innovation, with patients having greater control over their medical information.

3.5 Patient Concerns and Expectations Regarding Access to Medical Data

Patients have diverse views and concerns regarding medical data security, privacy, and unwanted access from others. Hassol et al. [23] conducted a study to explore patient experiences and attitudes about access to their electronic health records (EHRs) and linked web messaging. The findings revealed that patients had mixed views on medical data security and privacy. While some patients expressed concerns

about unauthorised access to their health information, others felt that the benefits of sharing data outweighed the potential risks [23].

Patients expect specific details from health providers regarding access to their medical data. Firstly, they expect access to their complete medical records, including diagnoses, test results, treatment plans, and medications [24]. They also expect timely and convenient access to their data through online portals or mobile applications [25]. Patients want their medical data to be presented in an understandable and user-friendly format, with clear explanations of medical terminology and the use of visual aids if necessary [24]. Additionally, patients expect to have control over their data, being able to share it with other healthcare providers or family members as needed while also maintaining privacy and consent [24]. They also desire to integrate patient-generated data, such as data from wearable devices or mobile apps, into their medical records. Lastly, patients expect health providers to use their medical data for shared decision-making, considering their preferences, values, and goals [26].

However, patients also have concerns regarding access to their medical data. One primary concern is the security and privacy of their information. Patients worry about unauthorised access, data breaches, and potentially misusing sensitive health data [27]. They also fear that errors or discrepancies in their medical records could impact their healthcare decisions and outcomes [3]. Trust and confidentiality are essential to patients, and they are concerned that increased access to their medical data may compromise these aspects [24]. Patients may also worry about potential stigma or discrimination if their medical data, primarily related to acute conditions or mental health, is accessed or shared without consent [25]. Some patients express concerns about a lack of control over their data, including who has access to it and how it is used [3]. Technical barriers and the digital divide can also be concerns, as some patients may struggle with accessing or navigating online portals due to limited digital literacy or disparities in technology access [24] [27].

Patients' perspectives and concerns significantly shape their interactions with healthcare providers and medical data. Addressing these can enhance patient-centred care, data quality, patient engagement, and healthcare outcomes. Privacy, digital literacy, unequal access to technology, and the fear of using sensitive data must be addressed. Patients desire comprehensive, accurate, and understandable access to their medical data while ensuring privacy and trust. They also expect healthcare providers to utilise their medical data for shared decision-making aligning with their preferences, values, and goals. A patient-centred approach in health data systems could improve healthcare delivery by understanding and meeting patients' expectations and alleviating their concerns.

4. The proposed architecture

A patient-centric, interoperable, and open architecture for personal health data management is becoming increasingly necessary in the changing healthcare landscape. The fast advancement of digital technologies and the growing demand for personalised healthcare demand a paradigm shift in how we handle health data. This chapter delves into the layered architecture design that aims to meet these needs, providing a comprehensive framework for integrating data from various sources, incorporating self-sovereign identity principles for secure access control, and ensuring privacy and security during data transfer, usage, and storage. Furthermore, it proposes a dedicated layer for building products and services on top of the architecture, placing the patient at the centre of their healthcare journey. The aim is to provide a blueprint for an architecture that can revolutionise personal health data management.

As we move towards designing an architecture that answers the needs of a patient-centric, interoperable, and open health data management system, it is crucial first to outline the fundamental principles.

- **Interoperability**: The architecture should allow seamless integration and communication between systems and data sources.

- **Openness**: The architecture should be based on open standards and protocols to avoid vendor lock-in and promote innovation.
- **Patient-centricity**: The architecture should put the patient at the centre, giving them control over their data and enabling them to actively participate in their healthcare journey.
- **Data Integration**: The architecture should be capable of incorporating and securely storing data from various sources, including electronic health records (EHRs), personal health records (PHRs), and wearable device data.
- **Identity Management**: The architecture should incorporate self-sovereign identity principles to ensure secure, privacy-preserving access control.
- **Privacy and Security**: The architecture should ensure the privacy and security of data in rest and transit.
- **Business Application Development**: The architecture should provide a layer for developing new business models by leveraging the entrepreneurial community to create new products and services that meet the patient's needs.

The architecture proposed herein is designed as a multi-layered structure, each addressing a specific principle. The layers include Data Storage, Identity and Access Management, including automation and Consent Management, Data Privacy and Security, Data Exchange and Interoperability, Analytics and AI Integration, Converging to the Business and Application Layer. A cross-cutting layer – Governance and Compliance to ensure the applicable privacy and security regulations and monitor performance, security and usability. Each layer comprises various components that interact with each other and with components of other layers, ensuring a seamless, secure, and efficient flow of information (figure below).

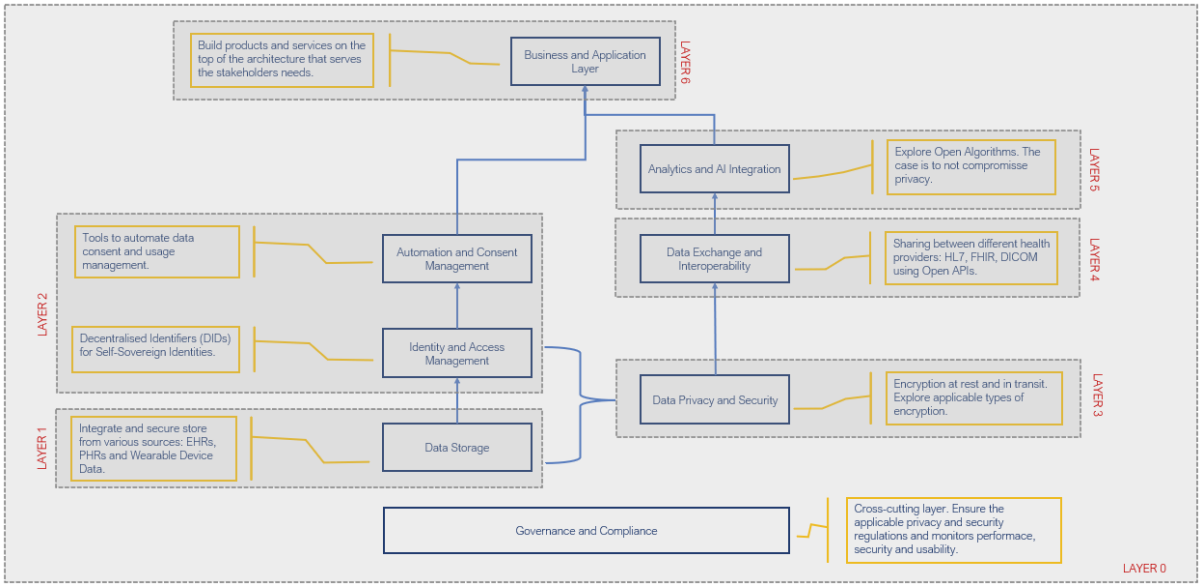

Figure 3 - The Proposed Multi-Layer Architecture.

1. **Data Storage Layer**: This is the foundational layer where all health data is stored, capable of integrating and securely storing data from multiple sources such as electronic health records (EHRs), personal health records (PHRs), and wearable device data. Components include databases, data warehouses, cloud storage or even decentralised structures such as IPFS. Each component interacts with each other and with components of other layers through secure, standardized APIs to ensure data consistency and integrity.

2. **Identity and Access Management Layer**: This layer manages user identities and ensures secure and privacy-preserving access control, incorporating automation and self-sovereign identity principles. The components include identity providers, authentication servers, access control, and consent automation mechanisms. They interact with the Data and Security Layer and Business and Application Layer to authenticate and authorise users and enforce access control policies with the Data Storage layer.
3. **Data Exchange and Interoperability Layer**: This layer facilitates communication between systems and data sources, leveraging open standards and protocols to ensure interoperability. Components include middleware and integration engines using standards like Health Level Seven (HL7), Fast Healthcare Interoperability Resources (FHIR), and Digital Imaging and Communications in Medicine (DICOM), using Open APIs.
4. **Analytics and AI Integration Layer**: This layer integrates analytics and AI capabilities, interacting with the Data Storage Layer to fetch data for analysis and prediction, with the Data Privacy and Security Layer and the Business and Application Layer to provide insights to applications. This layer includes data processing engines, machine learning algorithms, and AI models.
5. **Data Privacy and Security Layer**: This layer safeguards the privacy and security of data during transfer, usage, and storage. It incorporates the latest security technologies and adheres to all relevant regulations. Components include encryption mechanisms, secure data transfer protocols, and privacy-preserving technologies. This layer interacts with all other layers to ensure rest and transit encryption.
6. **Business and Application Layer**: This layer enables the development of products and services (applications) designed for patients enabling active participation in their healthcare journey. Components include patient portals, mobile health apps, and telemedicine platforms. These applications interact with the Identity and Access Management Layer for end-user authentication and authorization, the Data Exchange and Interoperability Layer for data exchange, the Data Storage Layer for data storage and retrieval and the Analytics and AI Integration to provide insights.

In summary, the proposed multi-layered architecture addresses the evolving needs of healthcare data management, focusing on interoperability, patient-centricity, and openness. It incorporates advanced analytics and AI capabilities and ensures governance and compliance. Each layer plays a critical role in ensuring a secure and efficient flow of information. The next step is to validate this architecture in the market, refining it based on real-world feedback and performance.

5. Conclusion and future research recommendations

This paper has explored the pressing need for an interoperable, open, and patient-centric global architecture for personal health data management. The rapid advancement of digital technologies and the increasing demand for personalised Healthcare demands a paradigm shift in handling health data. The proposed architecture, grounded in interoperability, openness, and patient-centricity principles, provides a blueprint for revolutionising personal health data management. The complexities of patient data ownership, data control, and privacy within the healthcare system have been highlighted, emphasising the importance of understanding these aspects to ensure the successful implementation of the proposed architecture. The potential ramifications of limited access and control over personal health data have been highlighted, revealing the critical nature of data ownership in the healthcare industry. The proposed architecture is designed to meet the evolving needs of healthcare data management, focusing on interoperability, patient-centricity, and openness while ensuring privacy, security, and governance. It aims to integrate data from various sources, incorporate self-sovereign identity principles

for secure access control, and promote the development of new business models (products, services and applications), placing the patient at the centre of their healthcare journey.

However, the journey towards this vision is weighed down with challenges. Future research should focus on validating the proposed architecture in the market and refining it based on real-world feedback and performance. It is also crucial to address patients' concerns, such as privacy, digital literacy, unequal access to technology, and the fear of using sensitive data. Moreover, the role of health information exchanges and the adoption of standards need further exploration. The nuances of laws and regulations affecting health data ownership across various geographies should be studied more deeply.

In conclusion, developing an interoperable, open, and patient-centric global architecture for personal health data management can revolutionise the healthcare industry and empower patients to take control of their health data. It is a challenging but necessary endeavour, and this paper hopes to contribute to the ongoing discourse and research in this area.

6. Conflict of Interest

The authors declare that the research was conducted without any commercial or financial relationships that could be construed as a potential conflict of interest.

7. Acknowledgments

Authors acknowledge Fundação para a Ciência e a Tecnologia (FCT, IP) for its financial support via the project UIDB/00667/2020 and UIDP/00667/2020 (UNIDEMI).

References

[1] Pillay R. Healthcare 3.0 - How Technology is Driving the Transition to Prosumers, Platforms and Outsurance. Xlibris Corporation; 2018.

[2] Healthcare Data Breach Statistics. The HIPAA Journal n.d. https://www.hipaajournal.com/healthcare-data-breach-statistics (accessed March 12, 2023).

[3] Kish LJ, Topol EJ. Unpatients—why patients should own their medical data. Nature Biotechnology 2015 33:9 2015;33:921–4. https://doi.org/10.1038/nbt.3340.

[4] Carvalho JV, Rocha Á, Vasconcelos J, Abreu A. A health data analytics maturity model for hospitals information systems. Int J Inf Manage 2019;46:278–85. https://doi.org/10.1016/j.ijinfomgt.2018.07.001.

[5] Awrahman BJ, Aziz Fatah C, Hamaamin MY. A Review of the Role and Challenges of Big Data in Healthcare Informatics and Analytics. Comput Intell Neurosci 2022;2022. https://doi.org/10.1155/2022/5317760.

[6] Vest JR, Grannis SJ, Haut DP, Halverson PK, Menachemi N. Using structured and unstructured data to identify patients' need for services that address the social determinants of health. Int J Med Inform 2017;107:101–6. https://doi.org/10.1016/j.ijmedinf.2017.09.008.

[7] Bhartiya S, Mehrotra D, Girdhar A. Issues in Achieving Complete Interoperability while Sharing Electronic Health Records. Procedia Comput Sci 2016;78:192–8. https://doi.org/10.1016/J.PROCS.2016.02.033.

[8] Torab-Miandoab A, Samad-Soltani T, Jodati A, Rezaei-Hachesu P. Interoperability of heterogeneous health information systems: a systematic literature review. BMC Med Inform Decis Mak 2023;23:1-1–13. https://doi.org/10.1186/s12911-023-02115-5.

[9] Interoperability in Healthcare | HIMSS n.d. https://www.himss.org/resources/interoperability-healthcare (accessed March 13, 2023).

[10] Ulriksen GH, Pedersen R, Ellingsen G. Infrastructuring in Healthcare through the OpenEHR Architecture. Comput Support Coop Work 2017;26:33–69. https://doi.org/10.1007/s10606-017-9269-x.

[11] Holmes JH, Beinlich J, Boland MR, Bowles KH, Chen Y, Cook TS, et al. Why Is the Electronic Health Record so Challenging for Research and Clinical Care? Methods Inf Med 2021;60:32–48. https://doi.org/10.1055/s-0041-1731784.

[12] Dixon BE, Holmgren AJ, Adler-Milstein J, Grannis SJ. Health Information Exchange and Interoperability. Clinical Informatics Study Guide, Springer International Publishing; 2022, p. 203–19. https://doi.org/10.1007/978-3-030-93765-2_14.

[13] Piasecki J, Cheah PY. Ownership of individual-level health data, data sharing, and data governance. BMC Med Ethics 2022;23. https://doi.org/10.1186/s12910-022-00848-y.

[14] Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al. Healthcare Data Breaches: Insights and Implications. Healthcare 2020;8:133. https://doi.org/10.3390/healthcare8020133.

[15] Jahnavi R. Data Breaches in Healthcare Security Systems. 2021.

[16] Windley JP. Learning Digital Identity - Design, Deploy, and Manage Identity Architectures. First Edition. O'Reilly Media Inc.; 2023.

[17] Eze B, Kuziemsky C, Peyton L. A Patient Identity Matching Service for Cloud-based Performance Management of Community Healthcare. Procedia Comput Sci, vol. 113, Elsevier B.V.; 2017, p. 287–94. https://doi.org/10.1016/j.procs.2017.08.321.

[18] Stewart BA, Fernandes S, Rodriguez-Huertas E, Landzberg M. A preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients. Journal of the American Medical Informatics Association 2010;17:341–4. https://doi.org/10.1136/JAMIA.2009.001750.

[19] Riplinger L, Piera-Jiménez J, Dooling JP. Patient Identification Techniques - Approaches, Implications, and Findings. Yearb Med Inform 2020;29:81–6. https://doi.org/10.1055/s-0040-1701984.

[20] IEEE Communications Society, Institute of Electrical and Electronics Engineers. 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). n.d.

[21] Zachariadis M, Ozcan P. THE API ECONOMY AND DIGITAL TRANSFORMATION IN FINANCIAL SERVICES: THE CASE OF OPEN BANKING. 2017.

[22] Basavaraj Kakade R, Veshne NA. UNIFIED PAYMENT INTERFACE (UPI)-A WAY TOWARDS CASHLESS ECONOMY. International Research Journal of Engineering and Technology 2017.

[23] Hassol A, Walker JM, Kidder D, Rokita K, Young D, Pierdon S, et al. Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging. Journal of the American Medical Informatics Association 2004;11:505–13. https://doi.org/10.1197/jamia.M1593.

[24] Ross SE, Todd J, Moore LA, Beaty BL, Wittevrongel L, Lin CT. Expectations of patients and physicians regarding patient-accessible medical records. J Med Internet Res 2005;7. https://doi.org/10.2196/JMIR.7.2.E13.

[25] Calvillo J, Román I, Roa LM. How technology is empowering patients? A literature review. Health Expectations 2015;18:643–52. https://doi.org/10.1111/hex.12089.

[26] Schroeder K, Bertelsen N, Scott J, Deane K, Dormer L, Nair D, et al. Building from Patient Experiences to Deliver Patient-Focused Healthcare Systems in Collaboration with Patients: A Call to Action. Ther Innov Regul Sci 2022;56:848–58. https://doi.org/10.1007/S43441-022-00432-X/FIGURES/2.

[27] Iacona S La, Militello C, Serbanati LD, Mastratisi MA, Ricci FL, Gilardi MC. Personal health system: A tool to support the patient empowerment. 2015 E-Health and Bioengineering Conference, EHB 2015 2016. https://doi.org/10.1109/EHB.2015.7391370.