Storage Standards and Solutions, Data Storage, Sharing, and Structuring in Digital Health

A Brazilian Case Study

Rodrigues de Oliveira, Nicollas; de Rezende dos Santos, Yago; Rocha Mendes, Ana Carolina; Nunes Nasseh Barbosa, Guilherme; Tuler de Oliveira, M.; Valle, Rafael; Scherly Varela Medeiros, Dianne; Mattos, Diogo Menezes Ferrazani

DOI
10.3390/info15010020

Publication date
2024

Document Version
Final published version

Published in
Information (Switzerland)

Citation (APA)
Rodrigues de Oliveira, N., de Rezende dos Santos, Y., Rocha Mendes, A. C., Nunes Nasseh Barbosa, G., Tuler de Oliveira, M., Valle, R., Scherly Varela Medeiros, D., & Mattos, D. M. F. (2024). Storage Standards and Solutions, Data Storage, Sharing, and Structuring in Digital Health: A Brazilian Case Study. *Information (Switzerland)*, *15*(1), 1-36. Article 20. https://doi.org/10.3390/info15010020

information

Review

Storage Standards and Solutions, Data Storage, Sharing, and Structuring in Digital Health: A Brazilian Case Study

Nicollas Rodrigues de Oliveira [1], Yago de Rezende dos Santos [1], Ana Carolina Rocha Mendes [1], Guilherme Nunes Nasseh Barbosa [1], Marcela Tuler de Oliveira [2], Rafael Valle [3], Dianne Scherly Varela Medeiros [1] and Diogo M. F. Mattos [1,*]

[1] LabGen/MídiaCom, PPGEET/TCE/IC/UFF, Universidade Federal Fluminense (UFF), Niterói 24220-900, Brazil; nicollas_rodrigues@id.uff.br (N.R.d.O.); yagorezende@id.uff.br (Y.d.R.d.S.); anamendes@id.uff.br (A.C.R.M.); guilhermenasseh@id.uff.br (G.N.N.B.); diannescherly@id.uff.br (D.S.V.M.)
[2] Department of Engineering Systems and Services, Delft University of Technology (TU Delft), 2600 AA Delft, The Netherlands; m.tulerdeoliveira@tudelft.nl
[3] Rede Nacional de Ensino e Pesquisa (RNP), Rio de Janeiro 22290-906, Brazil; rafael.valle@rnp.br
* Correspondence: menezes@midiacom.uff.br

Abstract: The COVID-19 pandemic has highlighted the necessity for agile health services that enable reliable and secure information exchange, but achieving proper, private, and secure sharing of EMRs remains a challenge due to diverse data formats and fragmented records across multiple data silos, resulting in hindered coordination between healthcare teams, potential medical errors, and delays in patient care. While centralized EMR systems pose privacy risks and data format diversity complicates interoperability, blockchain technology offers a promising solution by providing decentralized storage, ensuring data integrity, enhancing access control, eliminating intermediaries, and increasing efficiency in healthcare. By focusing on a Brazilian case study, this paper explores the significance of EMR standards, security challenges, and blockchain-based approaches to promote interoperability and secure data sharing in the healthcare industry.

Keywords: healthcare standards; blockchain

Citation: Oliveira, N.R.d.; Santos, Y.d.R.d.; Mendes, A.C.R.; Barbosa, G.N.N.; Oliveira, M.T.d.; Valle, R.; Medeiros, D.S.V.; Mattos, D.M.F. Storage Standards and Solutions, Data Storage, Sharing, and Structuring in Digital Health: A Brazilian Case Study. *Information* **2024**, *15*, 20. https://doi.org/10.3390/info15010020

Academic Editor: Shmuel Tomi Klein

Received: 26 November 2023
Revised: 23 December 2023
Accepted: 24 December 2023
Published: 29 December 2023

1. Introduction

The healthcare sector is a typical example where sharing personal data between organizations is essential, and access to these data is intrinsically distributed. Healthcare professionals in many organizations need to analyze patient data to perform their tasks. However, these data are typically stored in silos in distinct locations and different formats, making it difficult to share. Thus, the complexity of the medical system prevents the patient's entire medical history from being easily accessed when needed. In this way, much information is lost or exhaustively repeated, making the diagnosis and treatment of the patient difficult and harming the patient's journey.

According to research from the Johns Hopkins American Hospital, medical errors rank as the third leading cause of death in the United States, often stemming from systemic issues like poorly coordinated care [1]. Overcoming the challenge of coordinating patient care can be achieved through secure and accurate sharing of patients' data, granting healthcare teams access to comprehensive health histories, facilitating early diagnosis, and improving treatment efficacy. Achieving these benefits is made possible through standardized electronic medical records (EMRs) stored in computerized healthcare environments, containing vital personal information like diagnoses and treatments, distributed among hospitals and clinics where the patient received treatment. EMRs streamline patient data monitoring and access, enabling seamless care integration between medical teams and health facilities, thus providing patients with various levels of care with pertinent medical information. While

sharing these data benefits the patient, leading to more accurate diagnoses and appropriate treatments, it poses a significant challenge concerning privacy and security, given the highly sensitive nature of the information stored in EMRs. Often, patient data are shared without explicit consent among untrusted entities such as healthcare professionals, pharmacies, patient families, and other physicians [2]. Although efforts are made to share patient data through secure institutional medical systems, non-institutionalized and insecure means of communication are sometimes used for simplicity and immediacy. During the COVID-19 pandemic, there has been a notable emphasis on streamlining consultations and enhancing information exchange among patients, healthcare providers, and health organizations. Consequently, patient records have gained increased importance in public health [3], as they offer valuable data on diagnoses and prescribed medications, enabling identifying individuals belonging to COVID-19 risk groups, among other applications. The broader availability of patient data in electronic formats has significant implications for decision making and continuity of care in both the public and private sectors, fostering seamless data exchange between these realms. Timely data regarding disease outbreaks is crucial in effectively coordinating national-level public health policies and prevention strategies. Furthermore, the benefits of efficient data sharing extend to patients, who can access their information, including laboratory and imaging results, with the ability to port these data to other healthcare providers or organizations. Facilitating efficient and automated communication between patients and medical teams [4] enables universal access to data, promoting transparency and ultimately enhancing patient satisfaction.

The significance and relevance of data availability have been steadily increasing, with numerous establishments implementing this accessibility. In 2019, for instance, there was a notable rise in patient information in electronic format. Key improvements compared to 2018 included patient registration data (89% compared to 79%), the primary reasons for patient consultations (64% compared to 50%), and admission, transfer, and discharge records (56% compared to 43%) [5]. Notably, electronic systems in public establishments have seen remarkable growth in functionalities in recent years, particularly concerning the listing of all laboratory test results (from 17% in 2016 to 41% in 2019), patients using specific medications (from 18% in 2016 to 40% in 2019), and having medical prescriptions (from 29% to 51%) [5]. These improvements indicate an evolution in the level and complexity of adopted electronic systems, leading to reduced fragmentation in care provision, thus enhancing quality efficiency and minimizing gaps in care [6]. However, as data digitization practices advance and sensitive data generation increases significantly, the systems must address many challenges.

EMR systems predominantly rely on centralized client–server architectures, where a central authority holds full access to the entire system. However, this architecture brings forth particular challenges concerning privacy and security. System vulnerabilities can lead to failures and create opportunities for cyber attackers to breach patient data [7]. Managing these systems becomes a delicate task, requiring preserving privacy while ensuring data accessibility for authorized entities. Moreover, records are frequently stored in fragmented formats within local databases, hindering patients from accessing a comprehensive, consolidated electronic medical record [8].

Data format standardization is fundamental for achieving interoperability within the healthcare sector, entailing a unified language for exchanging and interpreting medical data and enabling diverse systems to communicate seamlessly. However, attaining such standardization presents notable challenges due to the escalating number of healthcare applications, EMRs, and medical devices, which have led to a rapid proliferation of varied data formats. This fragmentation poses substantial hurdles for healthcare professionals, researchers, and policymakers aiming to harness the power of data to enhance patient care, advance research endeavors, and facilitate evidence-based decision making.

Blockchain technology is emerging as a promising avenue for standardizing and achieving interoperability in EMRs. It aims to facilitate the verification and registration of EMRs through a consensus among peers participating in a peer-to-peer network. This

approach ensures reliable execution of data access policies, thereby upholding data integrity, accountability, and non-repudiation [9]. Blockchain technology becomes particularly appealing for applications requiring input from multiple stakeholders, where trust is challenging to establish using conventional technologies. Moreover, it addresses the issues of reliable activity tracking and data integrity while eliminating the need for intermediaries, resulting in enhanced overall system efficiency [10]. The healthcare sector stands as a promising candidate for leveraging blockchain's potential, owing to critical factors such as its potential to play a pivotal role in improving trust and transparency [11,12]:

- **Decentralization**: There is no need for an intermediary, and the database system is available to anyone connected to the network with the necessary access level. The monitoring, storage, access, and updating of data can be carried out in the various systems that are part of the network;
- **Transparency**: The data registered and stored in a blockchain are transparent to users, implying that all users can view the transactions carried out via blockchain;
- **Immutability**: Stored data cannot be modified, allowing stakeholders to prove with mathematical certainty that the historical data stream is accurate and unmodified [10];
- **Autonomy**: The network nodes are independent and autonomous, being able to access, transfer, store, and update data safely and without external intervention;
- **Anonymity**: The identity of the participants is anonymous, contributing to the privacy, security, and reliability of the system;

This paper comprehensively examines the main standards employed for storing and sharing EMRs, encompassing traditional ones, as well as emerging formats. Specific use domains are thoroughly explored, including storage, sharing, structure, and terminologies. By addressing security and privacy challenges in accessing medical data, this paper emphasizes access control mechanisms available on commercial and open-source platforms. These challenges encompass incompatible data models, varying terminology and coding systems, diverse implementation practices, and privacy and security concerns, necessitating harmonized policies and regulations across health data domains. The contributions of this work are twofold. Firstly, we provide a comprehensive overview of the primary standards and solutions implemented in the Brazilian healthcare system. Secondly, we delve into the advantages of incorporating blockchain technology to enhance legacy healthcare systems and address the main challenges associated with such adoption. The paper also delves into proposals utilizing blockchain technology for data sharing and access policy management, providing fundamental concepts for readers' understanding.

Figure 1 visually depicts the paper's structure. The solid arrows indicate the recommended sequence of sections for readers already familiar with basic blockchain technology concepts, while the dashed arrows point to a detour through Section 3, which provides an introduction to the fundamentals of blockchain technology.

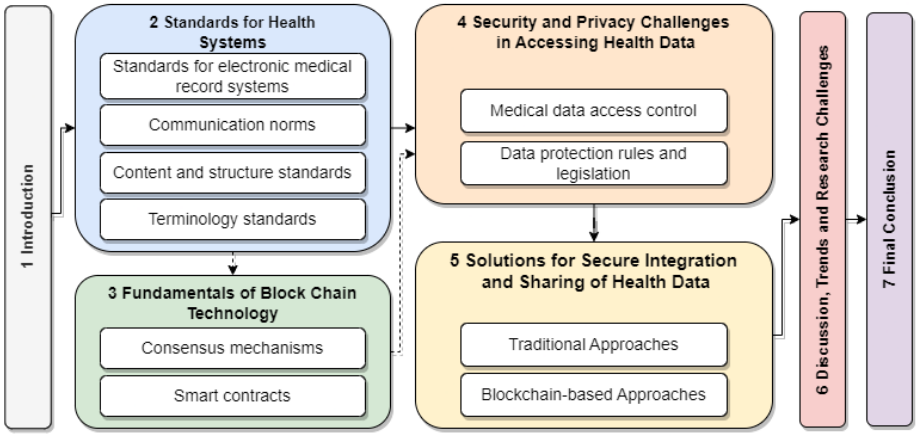

Figure 1. The structure of the paper.

2. Standards for Health Data Systems

Standards governing health data systems encompass a comprehensive set of norms, specifications, and guidelines designed to parameterize the collection, storage, processing, and sharing of clinical and administrative information within healthcare systems. Alongside standards for health systems, specific organizations contribute to standardizing communication methods between systems and structural norms for storing and representing clinical data, resulting in a diverse array of medical system standards worldwide.

Several global initiatives have pioneered these efforts to establish standards and guidelines that transcend borders and sectors. The Observational Medical Outcomes Partnership (OMOP) (available at https://www.ohdsi.org/data-standardization/ (accessed on 24 September 2023)) initiative focuses on standardizing observational health data. By creating a common framework for representing population health data, OMOP enables more consistent and comparative analyses, providing valuable insights into medical outcomes. Another influential global initiative is Integrating the Healthcare Enterprise (IHE) (available at https://www.ihe.net/ (accessed on 24 September 2023)), which aims to promote interoperability among healthcare information systems. By defining integration profiles based on established standards, IHE facilitates harmonizing diverse systems, enhancing collaboration and data exchange among healthcare entities. Although it is also a standard, which will be further detailed in Section 2.3, Health Level Seven International (HL7) is also known as a leading global organization in developing standards for exchanging electronic health information. With a comprehensive range of standards, HL7 is crucial in modernizing health information exchange, enabling more efficient and flexible communication. These initiatives represent significant collective efforts to create a more integrated and effective digital healthcare environment. This section addresses four critical areas of standards: (i) electronic medical record systems; (ii) content and structure; (iii) communication; and (iv) terminologies. Table 1 summarizes the patterns covered in this context.

Table 1. Patterns presented in this work.

Pattern Type	Pattern Name	Standardizing Entity
Electronic Medical Record	openEHR	openEHR
Content and Structure	CDA	HL7
	FHIR	HL7
	DICOM	NEMA
Communication	FHIR	HL7
	HL7 V2	HL7
	HL7 V3	HL7
	DICOM	NEMA
Terminology	TUSS	ANS, AMB, COPISS
	SNOMED CT	SNOMED International
	LOINC	Regenstrief Institute
	ICD	WHO

In Brazil, the healthcare system is predominantly represented by the Unified Health System (*Sistema Único de Saúde*—SUS), a public health system designed to provide comprehensive, universal, and accessible healthcare services to the entire population. The backbone of SUS is formed by basic health units (*unidades básicas de saúde*—UBSs), which serve as the primary entry point for individuals seeking healthcare services. UBSs play a pivotal role in preventive care, health promotion, and the management of common health issues. The territorial vastness and socioeconomic variations contribute to the complexity of healthcare provision in Brazil, marked by multiple healthcare standards. Thus, several Brazilian entities, such as the Ministry of Health (MS), the National Supplementary Health

Agency (*Agência Nacional de Saúde Suplementar*—ANS), the National Council of Health Secretaries (*Conselho Nacional de Secretários de Saúde*—CONASS), and the National Health Council (*Conselho Nacional de Saúde*—CNS), are responsible for the adoption and implementation of these standards. Simultaneously, international standards find widespread adoption in developing healthcare systems in various countries. Understanding and selecting these standards are pivotal to ensuring interoperability among diverse health systems available in the market, ultimately promoting enhanced efficiency, safety, and quality in healthcare services. It is worth noting that all standards detailed in this work are in the Brazilian healthcare context and, therefore, are included in the article's case study.

2.1. Standards for Electronic Medical Record Systems

Standards for electronic medical records systems are centrally focused on promoting interoperability between different health systems and applications, allowing the sharing and exchanging of health information securely, efficiently, and accurately. Such standards support the formulation of reference models aligned with laws and regulations and dedicated to developing new health applications.

The Open Electronic Health Record (openEHR) is an organization dedicated to developing and maintaining software system specifications and standards for EMRs. While it proposes health system models, it does not create its applications. Instead, its primary contributions consist of two reference architectures designed to integrate health software solutions. openEHR specifies various system components alongside the architectures, encompassing communication, storage, integration, and data representation (available at https://openehr.org/developers (accessed on 24 September 2023)). One distinctive feature of the openEHR specifications is the adoption of a role-based approach, delegating healthcare professionals to define procedures and the initial level of data representation in the model, referred to as "archetypes", which adapt to specific contexts. Concurrently, developers are responsible for integrating the components, designing graphical interfaces, and developing software services related to data handling. This separation of roles ensures an effective collaboration between healthcare professionals and developers in creating adaptable and efficient EMR systems.

openEHR first specifies a general model organized into components. Each component and its specificities are detailed in the standard definitions. The two reference architectures specified by openEHR are particularizations of this general model. Figure 2 shows the organization of the specifications into functional blocks of the general model proposed by openEHR (available at https://specifications.openehr.org/releases/BASE/latest/architecture_overview.html (accessed on 24 September 2023)). These blocks are organized as follows:

- **Conformity**: The model application's compliance criteria serve as a comprehensive guide for conducting system validation tests, encompassing areas such as bids, security rules, integration tests, and APIs. These criteria are typically applied to the implementation technology specifications (ITS), forming an essential framework to ensure adherence and compatibility with the intended model application;
- **Service platforms and application programming interfaces (APIs)**: Abstract formal APIs define the interfaces to the openEHR platform;
- **Formalisms**: The framework establishes versatile formalisms applicable to data querying and the definition of static data and procedures, incorporating archetypes as class libraries specifically structured for medical contexts with predefined objectives, yet designed for flexible reuse. Furthermore, it includes the Unified Modeling Language (UML) representation library for internal classes and the Archetype Query Language (AQL), serving as a portable query language tailored for archetypes;
- **Content**: Defines primary content templates for the openEHR platform, including demographics and electronic health records. Furthermore, it supports the openEHR terminology along with expressions of other terminologies;

- **Clinical decision support (CDS) processes and support**: Defines components of the clinical process and the CDS, containing the task planning specifications and the Guideline Definition Language (GDL), both used to develop manuals and usage guidelines organized by context in applications. The component is aimed at application users;
- **Foundation:** Defines primitive types, identifiers, and other fundamental classes for the operation of openEHR;
- **Implementation technology specification (ITS):** Defines components of the openEHR specification that focus on interoperability, such as the communication API and the various types of data encoding, such as JavaScript Object Notation (JSON) and XML Schema Definition (XSDs), in addition to the collection of model representations used to interface with other systems, such as the basic meta-model—BMM).

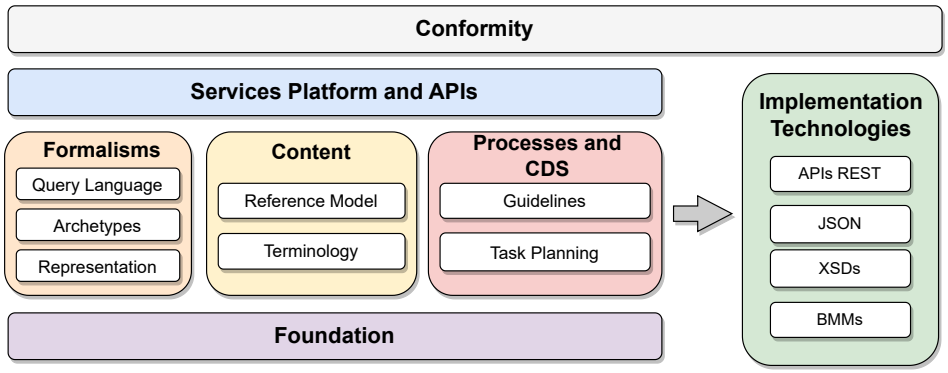

Figure 2. Organization of the components of the openEHR reference model specifications.

openEHR's initial reference architecture serves as a generic medical information system, providing a foundational framework for developing applications with assured interoperability. This achievement is made possible by defining all components based on standards established by openEHR and other groups like the HL7 organization, which sets communication and structure standards (Sections 2.2 and 2.3). Utilizing communication standards facilitates seamless data exchange among diverse systems, specifying formats, document architecture, data elements, content, methods, and APIs to achieve interoperability. In contrast, the second specified architecture is an integration system for diverse systems, acting as a standardization middleware for communication and data storage. Its primary objective is to integrate and standardize legacy systems, focusing on defining APIs between the various systems. The specifications enable the capture, storage, retrieval, and sharing of clinical information in a uniform format.

Given the dynamic nature of healthcare systems, the openEHR specifications are highly detailed, while the architectures and models remain generic. The specifications define the formalism of archetypes necessary to express domain content through templates and forms, ensuring adaptability to varying contexts. Additionally, openEHR defines an open application programming interface and a collection of predefined static models, including demographics and universal medical procedures, to streamline the development process for the intended systems.

2.2. Content and Structure Standards

Content and structure standards play a crucial role in determining the structure of electronic documents and the types of data they should contain within the healthcare domain. Content standards focus on specifying the patient data to be stored and how they relate to the steps of care. Such standards add semantic meaning to documents and generate historical information for continuous treatment. In contrast, structure standards aim to ensure data sharing between systems and enhance interoperability among healthcare facilities without prescribing the specific transmission format of these documents.

Expressed in XML format, the Clinical Document Architecture (CDA) is a notable standard that contains patient data and care context. Developed and maintained by the HL7 organization, a leading standards group for medical systems, the CDA standard consolidates various historical variations and defines the implementation standard for CDA documents [13]. The CDA is tailored both in terms of content and structure, and it is organized into templates based on specific use cases, making it less generic but suitable for scenarios requiring a hierarchical approach. As a result, the CDA standard is organized into use-case-based *templates*, currently having 12 different specifications. The implementation is object-oriented, contains all the features of this paradigm, and is suitable for cases requiring hierarchy.

Being the next-generation standards framework developed by HL7, Fast Healthcare Interoperability Resources (FHIR) focuses on standardizing electronic medical records' data representation and transactions. It is a set of rules and specifications based on key functionalities of traditional HL7 standards, including HL7 Version 2 (HL7 V2), HL7 Version 3 (HL7 V3), and the CDA. FHIR utilizes a building block called "resource" to represent interchangea ble data (available at https://www.hl7.org/fhir/structuredefinition.html (accessed on 24 September 2023)). Each resource follows a consistent format and contains various types of patient information, such as demographics, diagnoses, medications, allergies, and care plans. Resources are organized into sections and must include essential information, such as the type, an identifier, metadata, human-readable XHTML data summarizing the document, a reference to the document type in the system documentation, and standardized patient or examination data. FHIR allows representation in XML, JSON, and RDF formats, and it differs from the CDA as it is not limited to clinical information and does not require templates for interoperability. Instead, data interpretation is based on resource definitions, ensuring adequate data sharing. Additionally, FHIR employs a more expressive subset of XHTML than the CDA's XML-based syntax.

Figure 3 provides an example of an FHIR resource in XML format, highlighting its document structure sections, including resource identifier, version information, resource information in XHTML, and Uniform Resource Locator representation. The first section, in green, contains metadata and resource identification information. The following section, in purple, contains the human-readable summary, represented in XHTML format. The third section, in orange, contains additional information outside the basic definition of the Resource type. The last section, in blue, contains the record data.

Digital Imaging and Communications in Medicine (DICOM) is an international standard for the communication, storage, and representation of medical images and data derived from computed tomography, magnetic resonance imaging, and radiography, among other imaging examinations [14]. As traditional image file formats (JPEG, TIFF, BMP) are insufficient for accurate diagnosis, the standard adds information to the files necessary for diagnostic purposes. This information includes demographic data about the patient, acquisition parameters for the imaging study, image dimensions, color space, and a host of additional information to correctly display the image on the computer. This metadata inclusion allows the standardization of medical images and associated data and facilitates interpretation and diagnosis by healthcare professionals. Standardizing the file format and communication method allows media to be shared through services such as the picture archiving and communication system (PACS) and radiological information system (RIS), giving healthcare professionals more resources for clinical analysis.

The standard has been developed by a committee formed by the American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) and focuses on facilitating interoperability between medical imaging equipment. The committee specifies the network protocols for communication that equipment must use to transport data, the syntax and semantics of commands associated with data exchange in the context of medical imaging, a set of definitions for media storage services, and the specification of a proprietary file format and a standard for the structure of storage directories. All these specifications and definitions comprise the scope of the DICOM standard, which are

expressed in service–object pair (SOP) classes. These classes represent services, such as storage using network, media, or web, operating on types of information objects, such as CT or MRI images.

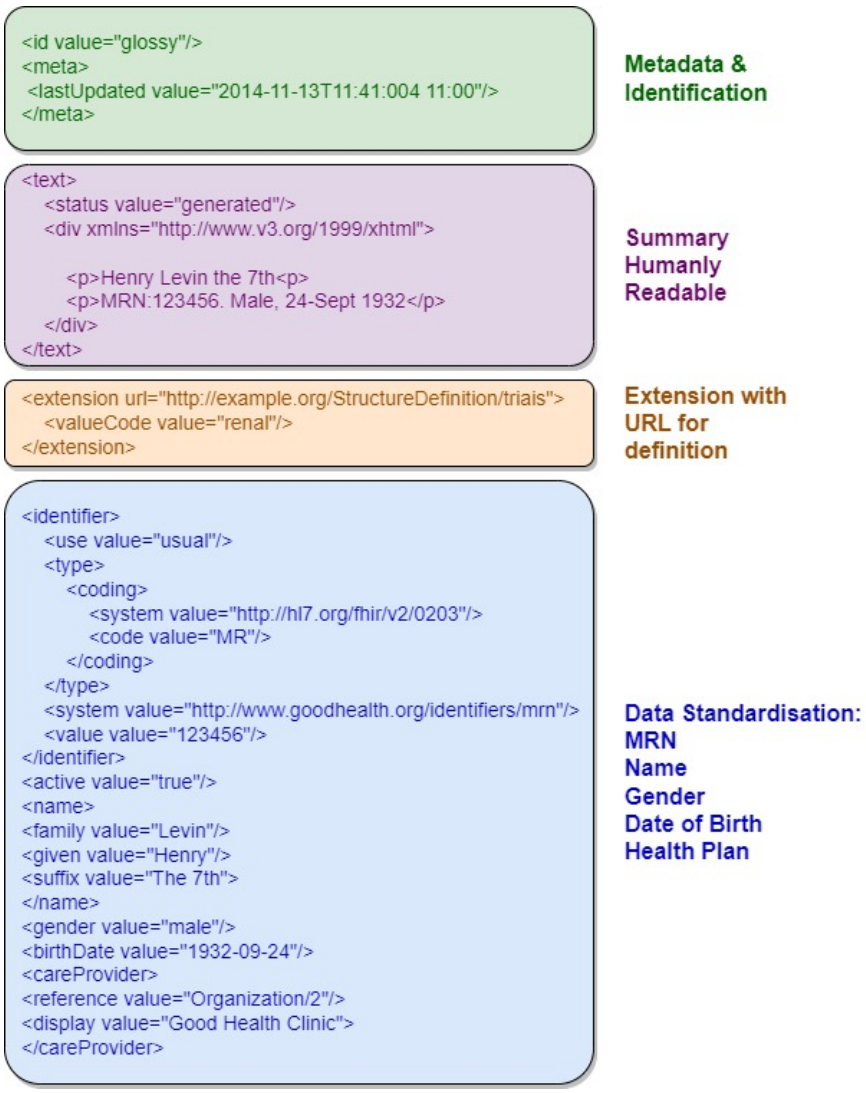

Figure 3. Example of an FHIR resource with the document structure sections highlighted.

Figure 4 illustrates the comprehensive model of DICOM services and functions, specifying their roles in transporting image data, associated information, real-time communication, and direct file access. The general service model encompasses functionalities for storing, providing access to, and processing DICOM images. This includes transactions of DICOM documents with outputs for message exchange, web services (REST API), real-time transmission, and file export to physical media. These functions are part of the DICOM application and are usually made available on an online server. At the bottom of the figure, the communication and transport protocols tailored for each service type are depicted. These protocols form the foundation for integrating systems that consume data from the DICOM application. This integrated approach ensures seamless interaction and interoperability across various DICOM services.

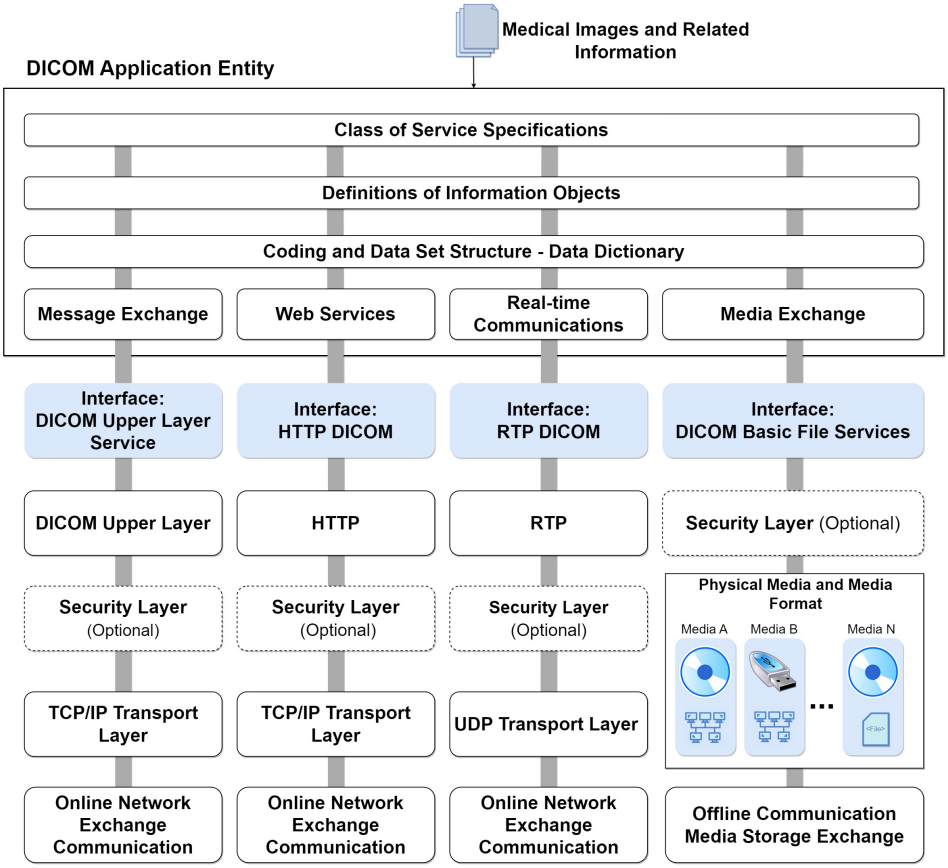

Figure 4. DICOM services model with integrated protocols.

2.3. Communication Standards

FHIR was designed to focus on flexible implementation, taking advantage of established web communication conventions, such as data representation using JSON, XML, and data exchange through HTTP-based RESTful APIs. The standard supports exchanging messages and documents in decoupled systems or with service-oriented architectures, generally meeting more modern trends for software development. Resources defined by FHIR are optimized for performing stateless transactions through RESTful APIs. Transactions of this type are the only ones currently defined by the FHIR specification. Transactions follow a simple "request" and "response" pattern. Requests and responses can occur to obtain an individual or batch payload. The payload is composed of a header and the content of interest. Reading a resource, for example, is achieved through a read request operation that sends an HTTP GET request to the resource URL (available at https://www.hl7.org/fhir/overview-dev.html (accessed on 24 September 2023)).

HL7 V2 (available at https://www.hl7.org/implement/standards/product_section.cfm?section=13 (accessed on)) is a standard for exchanging messages in the context of medical applications, whose main function is to define standards for the content or body of messages, a protocol for sending and receiving messages and defining different context requests, such as history requests and demographic data, among others. The HL7 V2 messaging framework is based on an event-based messaging paradigm. HL7 V2 defines the communication syntax at a low level, without worrying that messages are human-readable, by enclosing the entire message content in a string of characters. Figure 5 depicts the message content based on the HL7 V2 standard (available at https://www.ringholm.com/docs/04300_en.htm (accessed on 24 September 2023)), showing that a vertical bar sign separates data "|", wherein the data identifier is on the left side while the value is on the right. However, recent HL7 V2 versions use XML as an alternative encoding format.

Thus, the choice of which data and values must be in the message depends on the context of the request and its respective flow. Figure 6 shows the message flow for transferring immunization information from one health information system to another. The issuing system could be an EMR system, an immunization information system (IIS), or another type of health information system. An event such as an update or new record inserted in the issuing system initiates the creation and sending of a VXU message (vaccination update) containing an updated immunization record. The receiving system processes the message according to the used profile, applying local business rules. After successful processing, the receiver sends an acknowledgment message (aAcknowledgement—ACK) and adds the new record to the receiving system [15].

```
MSH|^~\&|GHH LAB|ELAB-3|GHH OE|BLDG4|200202150930||ORU^R01|CNTRL-3456|P|2.4<cr>
PID|||555-44-4444||EVERYWOMAN^EVE^E^^^^L|JONES|19620320|F|||153 FERNWOOD DR.^
^STATESVILLE^OH^35292||(206)3345232|(206)752-121||||AC555444444||67-A4335^OH^20030520<cr>
OBR|1|845439^GHH OE|1045813^GHH LAB|15545^GLUCOSE|||200202150730||||||||
555-55-5555^PRIMARY^PATRICIA P^^^^MD^^|||||||F||||||444-44-4444^HIPPOCRATES^HOWARD H^^^^MD<cr>
OBX|1|SN|1554-5^GLUCOSE^POST 12H CFST:MCNC:PT:SER/PLAS:QN||^182|mg/dl|70_105|H|||F<cr>
```

Figure 5. Example of a glucose test result message in HL7 V2 standard.

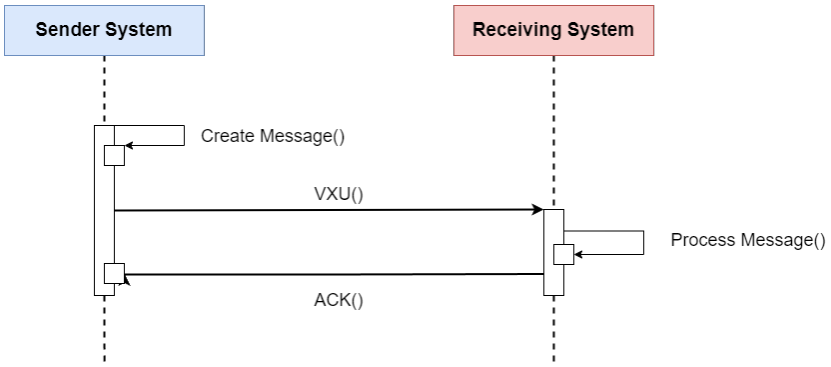

Figure 6. Sequence diagram of the flow specification for updating a patient's immunization history using the HL7 V2 standard. Adapted from [15].

The **HL7 V3** (available at https://www.hl7.org/implement/standards/product_brief.cfm?product_id=186 (accessed on 24 September 2023)) differs from HL7 V2 by incorporating a reference information model (RIM) to configure the message format in object-oriented modeling. In HL7 V3, messages are encoded into a mapping of classes of information needed for the context of medical applications. Each class receives its unique object identifier (OID) to ensure the universality of the specification of each object in its context. The specifications present attributes already known in HL7 V2, such as demographics, relationships, and data exchange flows like state machines. However, with the use of RIM, HL7 V3 also gains specifications for subsets of classes of RIM. In HL7 V3, the classes are organized and reused for different medical contexts, which is also part of the standard specification. Consequently, the HL7 V3 standard was organized in a context-oriented manner, or domain specification, which are sets of RIM classes that form a group applied to some area of the medical systems domain, such as attendance, exams, billing, emergency service, known as the domain message information model (D-MIM).

All the flows, communication protocols, and terminologies adopted for HL7 V2 form the basis for HL7 V3, which focuses on specifying the encoding of messages using XML and its syntax. In this way, the pattern becomes more intelligible and easier to implement. Figure 7 presents an excerpt of the same message (available at https://www.ringholm.com/docs/04300_en.htm (accessed on 24 September 2023)) shown in Figure 5, but structured according to the HL7 V3 standard. The example shows a patient's glucose test result and additional information that adds semantics to the data hierarchically.

```
<observationEvent>
  <id root="2.16.840.1.113883.19.1122.4" extension="1045813"
     assigningAuthorityName="GHH LAB Filler Orders"/>
  <code code="1554-5" codeSystemName="LN"
      codeSystem="2.16.840.1.113883.6.1"
      displayName="GLUCOSE^POST 12H
CFST:MCNC:PT:SER/PLAS:QN"/>
  <statusCode code="completed"/>
  <effectiveTime value="200202150730"/>
  <priorityCode code="R"/>
  <confidentialityCode code="N"
    codeSystem="2.16.840.1.113883.5.25"/>
  <value xsi:type="PQ" value="182" unit="mg/dL"/>
  <interpretationCode code="H"/>
  <referenceRange>
    <interpretationRange>
      <value xsi:type="IVL_PQ">
      <low value="70" unit="mg/dL"/>
      <high value="105" unit="mg/dL"/>
     </value>
     <interpretationCode code="N"/>
    </interpretationRange>
  </referenceRange>
```

Figure 7. Example of a patient glucose test result message in the HL7 V3 standard.

To standardize image representation, DICOM specifies a protocol for exchanging messages. The protocol provides a communication framework for DICOM services and is compatible with TCP and IP protocols. This compatibility enables communication over the internet between different applications that implement the DICOM standard. The DICOM communication protocol was developed based on the model open systems interconnection (OSI) reference model and implements functionalities of the application, presentation, and session layers (available at https://docs.oracle.com/cd/E57425_01/121/IMDCM/ch_intro.htm#IMDCM13799 (accessed on 24 September 2023)). An application that uses the DICOM protocol is called an application entity (AE). Each AE can request or provide one of the services of the DICOM protocol, called classes of services. Each service class consists of data and a function related to those data. Each service class consists of data and a function related to those data. For example, an MRI image can be associated with different functions, such as printing or storing. When an AE requests a service, it plays the service class user (SCU) role, and when the AE provides the service, it plays the service class provider (SCP) role. Communication between two AEs requires the establishment of a session called an "association". Establishing the association starts with exchanging important information, such as supported data encoding and the services provided by the SCP. After association, the SCU can request classes of service from the SCP. After sending the service classes, the association is finalized [16]. Despite specifying a communication standard, the DICOM communication protocol is not generic, only being capable of exchanging DICOM messages.

2.4. Terminology Standards

Terminology standards are crucial in ensuring clarity and consistency of medical information across various systems, promoting interoperability among medical record systems. These standards establish a comprehensive set of codes and classification systems to represent health concepts, aiming to achieve a unified and standardized form of representation [17].

In Brazil, the ANS collaborated with the Brazilian Medical Association (*Associação de Magistrados Brasileiros*—AMB) and the Coordination of Information Systems for Health (*Comitê de Padronização das Informações em Saúde Suplementar*—COPISS) (note from ANS http://www.ans.gov.br/images/stories/Plano_de_saude_e_Operadoras/Area_do_consumidor/nota13_geas_ggras_dipro_17012013.pdf (accessed on 24 September 2023)) to develop the Unified Terminology for Supplementary Health (*Terminologia Unificada da Saúde Suplementar*—TUSS),

which serves as a coding standard for medical procedures used in private health plans. The TUSS table defines medical procedures' nomenclature and corresponding identifier codes, groups, and subgroups. To facilitate seamless integration of this standard into healthcare provider systems, the ANS has made the TUSS standard available as a spreadsheet in xlsx format (available at https://www.gov.br/ans/pt-br/arquivos/assuntos/consumidor/o-que-seu-plano-deve-cobrir/correlacaotuss-rol_2021_site.xlsx (accessed on 24 September 2023)). By providing the terminology in this format, TUSS enables users to swiftly search for procedure codes, utilizing the standardized procedure names and available tools within electronic spreadsheet software. Moreover, the table format expedites the incorporation of new standard updates into databases, enabling integrated systems to stay up to date quickly.

The Systematized Nomenclature of Medicine—Clinical Terms (SNOMED CT) (available at https://www.snomed.org/five-step-briefing (accessed on 24 September 2023)) is a multilingual clinical terminology standard used to represent medical concepts in healthcare systems, with a focus on integrating terminologies from multiple countries. The standard has a broad scope, with more than 350,000 medical concepts specified in its terminology. To organize this vast collection of concepts, the standard organizes terms into three components:

- **Concepts:** Unique and computable identifier, used to guarantee the uniqueness of each term;
- **Descriptions:** Description of a uniquely and completely captured clinical idea called a fully specified name—(FSN), together with a set of synonyms that store the term name information in the multiple languages supported by the standard;
- **Relationships:** Records relationships between concepts, which can be of different types specified by the pattern. Relationships can represent a hierarchy between concepts, so that a concept always has at least one "is a" relationship, which defines its type.

In addition to specifying terminology, SNOMED CT specifies implementation forms for storing terminology data in systems, also serving as a basis for aiding in developing medical applications. Despite being a non-profit foundation, SNOMED charges a fee for membership in the organization and access to terminology if the user comes from a region without federated bodies to the foundation (available at https://www.snomed.org/get-snomed (accessed on 24 September 2023)).

The Logical Observation Identifiers Names and Codes (LOINC) aims to eliminate ambiguity in the clinical records' observation fields, proposes a comprehensive terminology for various types of observations related to exam and laboratory test results. It has emerged as a widely used database for categorizing and identifying observations from laboratory tests and clinical data, encompassing clinical observations, questionnaires, and other health assessments. This standard establishes a set of numerical codes and standardized names, facilitating efficient communication and data sharing between different healthcare systems. In contrast to other terminologies, LOINC's primary objective is to create distinct codes for each type of test, exam, and observation to be utilized in the observation fields of communication standards, such as HL7 V2. Furthermore, LOINC enhances traditional terminologies with semantics, enabling their combination to expand the capacity for specifying and exchanging information in medical records messages.

To achieve its goal, LOINC employs a logical framework consisting of six specification dimensions: (i) component (or analyte), representing the substance or entity being measured or observed; (ii) property, representing the characteristic or attribute of the analyte; (iii) time, representing the time interval during which an observation was made; (iv) system, representing the specimen or substance on which the observation was performed; (v) scale, defining the quantification or expression of the observation value; and (vi) method (optional), representing a high-level classification of how the observation was conducted, generally employed when the technique influences the clinical interpretation of results. This systematic categorization ensures clarity and consistency in defining and communicating

various observations, contributing to seamless data exchange and enhanced interoperability in the healthcare domain.

The confluence of the six formalization dimensions yields the FSN, which, in conjunction with the numerical identifier, constitutes the comprehensive definition of the observation type within LOINC. Alongside the FSN, LOINC provides more extended human-readable versions known as the long common name (LCN) and a condensed version termed the short name, typically utilized in tables or reports. Despite the specification and definition of FSNs for observations, messages only transmit the specified code. To obtain the code's definition, reference to the LOINC database is essential, utilizing the numerical code through the LOINC FHIR API (available at https://loinc.org/fhir/ (accessed on 24 September 2023)), the official website, or integrating the complete base into the system. An illustrative example of the process for specifying an observation related to manually counting white blood cells in a cerebral spinal fluid (CSF) sample is presented in Table 2 (example taken from LOINC's official website, available at https://loinc.org/get-started/loinc-term-basics/ (accessed on 24 September 2023)). This table exemplifies the steps LOINC employs to uniquely categorize diverse clinical observations, culminating in a textual identifier that fully encapsulates the observation's contextual value. The FSN, distinguished in light gray and bold, is formulated by combining the six components specified by the standard. The long and short versions of the name are also depicted in light gray lines within the table.

Table 2. LOINC 806-0 white blood cell count example.

Step	Value
ine Analyte	Leukocytes
Property	NCnc (*Number concentration*)
ine Time	Pt (*Point in time*)
ine System	CSF
Scale	Qn (*Quantitative*)
ine Method	*Manual Count*
ine FSN	Leukocytes: NCnc: Pt: CSF: Qn: Manual count
ine LCN	Leukocytes [#/volume] in Cerebral spinal fluid by Manual count
ine Short Name	WBC # CSF Manual

The World Health Organization (WHO) has developed the **International Classification of Diseases (ICD)**, now in its 11th edition, known as ICD-11, to enhance the statistical survey of causes of death and morbidity worldwide. This classification system plays a pivotal role in large-scale decision-making processes, intelligently influencing government planning and resource allocation. Consequently, data-driven planning significantly improves the quality of health services provided to the population [18]. The ICD-11 constitutes a systematically organized database, offering categories for diseases, disorders, health-related conditions, external causes of illness or death, anatomical details, environmental factors, activities, medications, vaccines, and other health-influencing information. Each classification level within the base is precisely specified according to its respective categories and assigned unique and sequential alphanumeric identification codes, establishing a hierarchy of related diseases [19].

For queries in the ICD-11 database, WHO provides three main components: a REST API over HTTP, a web graphical user interface (available at https://icd.who.int/browse11/l-m/en (accessed on 24 September 2023)), and a coding tool where users can assemble the correct ICD-11 code for a disease and its additional information. The tool is helpful for testing and validating software that uses the ICD-11 coding system. Figure 8 shows

the web interface of the ICD coding tool, highlighting an ICD-11 code generated just by selecting the characteristics of a disease. The user can search for keywords and select the desired combination of factors for a record. The example shows the code generated for the COVID-19 disease confirmed by a laboratory test, with the virus in its SARS-CoV-2 Omicron variant, with the patient in isolation.

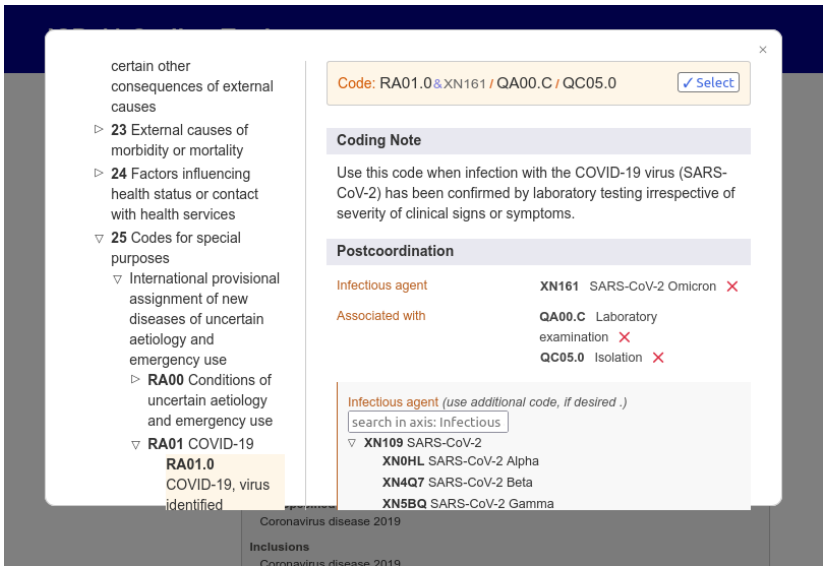

Figure 8. ICD-11 web application provided by the WHO presenting a negotiation tool.

3. Fundamentals of Blockchain Technology

Blockchain comprises a technology composed essentially of two essential elements: a data structure for chaining the blocks and a peer-to-peer network (peer-to-peer—P2P) capable of storing transactions in an orderly and distributed manner. As a central differential, blockchain technology enables the development of secure distributed applications in scenarios marked by mutual distrust between entities while dispensing with the need for a third centralizing entity, acting as a trust anchor to ensure security between transactions on the network [20]. Given these characteristics, the blockchain is commonly interpreted as a ledger distributed across several terminals in a network. Blockchain networks can be classified into different types: public, private, permissioned, and non-permissioned. Public networks have open content and no access control mechanism, allowing nodes to participate and generate new blocks without affecting consensus. In contrast, private networks have closed content and strict access controls to limit node participation. Permissioned networks treat all nodes equally, while in non-permissioned networks, nodes can perform different functions based on application needs, such as block mining and participating in the consensus mechanism.

Blockchain technology provides tamper resistance by requiring the manipulation of all subsequent blocks to alter data in a single block. Its decentralized nature eliminates a single point of failure, ensuring security and privacy even in conflicts of interest between parties involved in transactions. Nodes in the peer-to-peer network access an identical replica of the blockchain stored locally, ensuring data consistency through validation and consensus mechanisms [21]. Consensus is crucial to agree on the transactions inserted in a block and their execution order. Each block contains a cryptographic summary of the previous block, making it unlikely for a single node to modify block content. This cryptographic concatenation ensures the blockchain's integrity, consistency, and immutability, preserving the transaction history and preventing data removal or alteration. Asymmetric cryptography guarantees the veracity and non-repudiation of stored data, while pseudo-anonymity is maintained for parties involved in transactions, as their identities are concealed from the network [22]. Among the main consensus mechanisms for blockchains employed in the healthcare sector are:

- **Proof of work (PoW)**: A probabilistic consensus mechanism that implements logic based on competition between miners. Miners are nodes that seek to solve a complex cryptographic challenge so that the chosen transactions are recorded in a block inserted in the blockchain. In the PoW consensus mechanism, the resolution of the cryptographic challenge involves a brute-force approach, wherein miners exhaustively attempt different numeric values until they discover the specific cryptographic nonce. This nonce and the selected transactions are appended to the candidate block intended for inclusion in the blockchain. Subsequently, the candidate block is distributed across the network to be validated by other nodes. As an incentive for participating in the resource-intensive process of solving the challenge, miners are rewarded when they or their group successfully find the nonce and validate the block [23]. In PoW, the likelihood of a node being able to mine a block is directly tied to the computational power of the node, with more powerful nodes having a higher probability of successful mining.
- **Proof of stake (PoS)**: Represents another probabilistic consensus mechanism wherein the likelihood of successfully mining a block is contingent upon the active participation of nodes in the network. In PoS, mining nodes compete to discover a cryptographic digest value that is less than or equal to a predefined target value, thereby enabling them to mine a block. However, the complexity of finding the cryptographic digest is inversely proportional to the node's accumulated wealth, also known as the coin age. Coin age is quantified as the node's available resources multiplied by the time the node has held those resources. Consequently, the node with the highest level of participation and accumulated wealth stands a greater chance of validating the subsequent block [24].
- **Proof of authority (PoA)**: A consensus mechanism widely embraced in private networks, characterized by a designated entity responsible for appointing a set of authoritative nodes. These authoritative nodes hold the responsibility of generating new blocks and validating transactions. Consequently, any candidate block's inclusion in the blockchain necessitates prior validation and endorsement by at least one authoritative node. The decentralized nature of the network is upheld through unanimous agreement among the authority nodes regarding the global state of the blockchain. Specific platforms implement a rotating block generation scheme to prevent conflicts and resource wastage, ensuring each authority node receives an exclusive time interval for block generation. In case of any failures among authority nodes, the platform must detect and respond by removing the authority of the faulty node and disregarding any blocks mined by it [25].
- **Raft**: This consists of the main consensus mechanism used in Hyperledger Fabric (available at https://www.hyperledger.org/use/fabric (accessed on 24 September 2023)), recommended for production environments [26]. It is a fault-tolerant stopping mechanism and is based on the leader–follower model. Raft achieves consensus through the election of a leader, log replication, and security stages. Nodes can be in three states: candidate, follower, or leader. Initially, nodes are followers, and if no leader is detected, an election takes place. The leader communicates with clients, maintains a follower state, and replicates log entries. The leader uses a remote procedure call AppendEntries to replicate logs and validate the state of the follower. Raft ensures that transactions are entered in the same order across nodes and that the elected leader has the most recent logs. Raft offers advantages such as easy implementation in most common programming languages and an efficient election system. However, it requires significant storage capacity and has limitations such as the lack of Byzantine fault handling (Byzantine failure refers to the behavior of a node that deviates from the expected behavior of the defined protocol).
- **Practical Byzantine fault tolerance (PBFT)**: A deterministic consensus mechanism widely used in distributed systems and blockchain platforms such as Zilliqa and Hyperledger Fabric. The mechanism deals with failures in sending messages and delays in networks, assuming independent failures and partial dependence between

nodes. PBFT guarantees security and liveliness even with up to $(n-1)/3$ malicious nodes out of a total of n nodes. The algorithm involves four steps: (i) the client sends a transaction request to the leader; (ii) the leader forwards it to other nodes; (iii) these nodes execute the request; and (iv) sends a response to the client that expects $2f+1$ consistent responses, where f is the maximum tolerated number of failed responses. PBFT deals with faulty leaders through alternation-based (round-robin) lead exchange. The mechanism has the advantages of low energy consumption and fast execution time compared to other mechanisms resistant to Byzantine faults. However, it has limitations in more extensive networks due to increased message exchange and vulnerability to impersonation attacks (Sybil). PBFT is a practical consensus mechanism that ensures reliable communication and agreement between nodes while mitigating the impact of malicious nodes [26].

First introduced on the Ethereum trust computing platform, the smart contract consists of a self-executing application stored on the blockchain, translating the clauses of an actual contract into code. Through a known and accessible address, the smart contract has content that all network participants can inspect. Internally, a smart contract contains contractual rules agreed between the parties, which make the violation computationally prohibitive and, therefore, not advantageous to potential violators. In contrast to non-deterministic contracts, which make consensus unfeasible due to the randomness of the results achieved by different network nodes, smart contracts are naturally deterministic [9,20], which guarantees the convergence of the network overview. Since all interactions with a contract take place via signed messages, it is possible to track all participants involved in the operation of the contract. Contract triggering can be triggered by any change in state or transaction record on the blockchain, facilitating negotiation, validation, and trade execution without the need for third parties [22]. Due to the immutability of the blockchain, any mistakes made in the code of an already implemented smart contract are not amenable to correction. Furthermore, changes in the circumstances related to the performance of the contract, such as changes in laws and regulations, are equally complex to be accounted for by the contract already implemented. These changes require extensive and potentially costly reviews of the smart contract code by experts.

4. Security and Privacy Challenges in Accessing Health Data

In Brazil, the ConectaSUS Health Universal System (*Sistema Único de Saúde*—SUS) (available at https://conectesus.saude.gov.br/home (accessed on 24 September 2023)) application is responsible for providing health information in the country. On the platform, citizens can be able, through a mobile device or web access, to view their clinical history, including vaccination records, laboratory test results, and medications used, among other information. According to the World Bank, in 2022, Brazil was recognized as the country in the world with the second greatest maturity in digital government (available at https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2022/11/brasil-e-reconhecido-como-segundo-lider-em-governo-digital-no-mundo (accessed on 24 September 2023)). Currently, 80% of the Brazilian population, corresponding to approximately 140 million users, already have access to these platforms. Between 2009 and 2019, there were over 3000 healthcare data breaches in the United States, each involving at least 500 patient records. In 2019, 572 violations involving more than 41 million Americans were reported [27]. With the improvement in artificial intelligence models, patient data can be used for training on centralized servers with few layers of security, facilitating attackers' improper manipulation of this information [28]. This training, without proper safety rules, can affect hospitals that share data with research entities [29], since they are responsible for keeping these data.

Numerous well-known and widely exploited cyber-attacks on computer systems, including distributed denial of service (DDoS), phishing, ransomware, and social engineering, are also applicable in the context of electronic medical records. The primary motivation of attackers revolves around the lucrative trade in personal data and, in some instances,

espionage linked to the theft of patents and industrial intellectual property. Negligence and naivety exhibited by users often become crucial factors leading to the compromise of entire infrastructure and systems, irrespective of the attackers' intentions. Instances of weak passwords, sharing of credentials, and inattentive access to websites and web addresses can swiftly lead to the leakage of personal data. Thus, establishing mechanisms ensuring electronic medical records' transparency, confidentiality, and integrity is paramount in the present landscape. Promising technologies such as blockchain and smart contracts should serve as guiding principles in shaping the future of computer security in the healthcare domain.

One of the essential concerns when handling EMRs is that these data are private and belong to patients but are fully controlled by health institutions [30]. Another concern is related to identity management (IM), as it increases the trust and privacy in EMR [31]. IM for electronic medical record storage and query systems tends to be centralized, introducing a single point of failure and an access bottleneck for the entire system [2]. Therefore, although there are different blockchain-based proposals for storing and sharing electronic records [2,32,33], there is an opportunity for improvement for offering a service safer and adapted to the pains of the market. EMR systems are commonly implemented with poor security practices, potentially compromising the privacy and confidentiality of patient data [34]. In addition, sharing data for commercial purposes can also undermine trust in health plans and operators. EMR systems contain information considered highly confidential for many reasons; therefore, there is a strong need for confidentiality. The integrity of medical records becomes essential, as incorrect treatment based on erroneous data can be fatal. Furthermore, availability is as essential as integrity, as system information must be available for proper treatment at any time [35]. The main purpose of an EMR system is the availability of patient data. In this sense, access control should not prevent any legitimate request on behalf of the vital interest of patients [36].

4.1. Medical Data Access Control

Role-based access control (RBAC) stands as a prominent approach for access control, where each user can be assigned one or more roles, such as administrators, doctors, or patients, each carrying distinct access permission profiles. Administrators typically assign specific roles to users, and each role encompasses varying permissions. Figure 9 illustrates the RBAC access control model, where the system administrator defines roles and permissions. Users are then assigned one or more roles, each associated with specific permission levels in the system. However, systems adopting this model may compromise security due to the intricacies involved in managing groups and users, leading to the potential granting of permissions without genuine necessity. In the context of electronic medical records, the challenge lies in determining the specific situation in which a patient finds themselves at any given time, be it a regular consultation or emergency care. In emergencies, data access must be allowed on an exceptional basis.

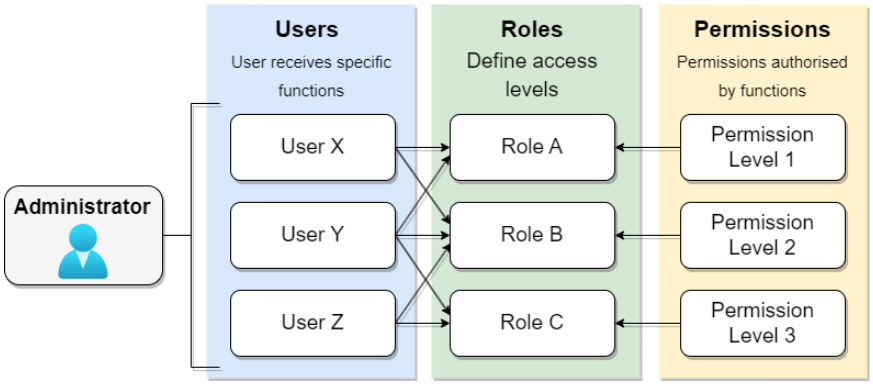

Figure 9. RBAC model.

Nevertheless, RBAC needs more flexibility to accommodate unpredictable scenarios, such as emergencies. Consequently, instances may arise where a patient requires care, but the attending doctor lacks the credentials to access the essential data, potentially compromising the quality of care. To address this limitation, some studies propose an **emergency role-based access control** (E-RBAC) variation. In E-RBAC, emergency roles are defined based on the requesting user's access level, enabling data querying in emergencies [37]. Despite RBAC being utilized in various access control approaches, its scalability poses challenges, as the indiscriminate increase in roles and policies may lead to management complexities [38].

Another access control approach is called **situation-based access control (SitBAC)** [39]. SitBAC offers an alternative approach to access control, shifting the focus from users' roles to the patient's current situation. Unlike RBAC, which separates users from permissions based on predefined roles, SitBAC grants data access permission per request. This approach recognizes that accessing patient data is contingent on various factors that constitute the access situation, including the data requester's identity, the task to be performed, legal authorization, and more. However, the integration of SitBAC with RBAC is not explicitly defined, and SitBAC fails to address fundamental security concerns such as confidentiality, integrity, and non-repudiation [38].

The **work-based access control** model (WBAC) centers on the tasks to be performed by professionals and their teams. In this model, a user's privileges are dynamically adjusted according to the specific treatment they are assigned to undertake. A separation of duties mechanism prevents fraud by ensuring a user can only hold one team role at a given time. The WBAC model involves users assigned to roles or teams, team members associated with team roles, and the specific tasks that can be assigned to each team. Permissions can be associated with individual roles and team roles. However, one of the primary challenges of WBAC is managing tasks for each user, which can lead to increased complexity and errors in task assignment [40,41].

Attribute-based access control (ABAC) is a paradigm wherein access rights are granted based on policies involving logical attribute combinations. Users must be registered in a central identity management (IM) system, such as Lightweight Directory Access Protocol (LDAP) or Active Directory (AD), and associated with the predefined attributes shown in Figure 10. These attributes encompass user-, resource-, and environment-related information. The ABAC policies, requests, and responses are expressed in the XACML language. A policy comprises a set of rules that the requestor must adhere to, and the evaluation of these rules using attribute values yields the response, determining the access decision. While the ABAC model offers greater granularity in accessing patient information, its application in real health scenarios, especially during intensive care, poses challenges due to data sharing between organizations. This limitation may leave intensive care without adequate access protection in existing ABAC-based access control models [36].

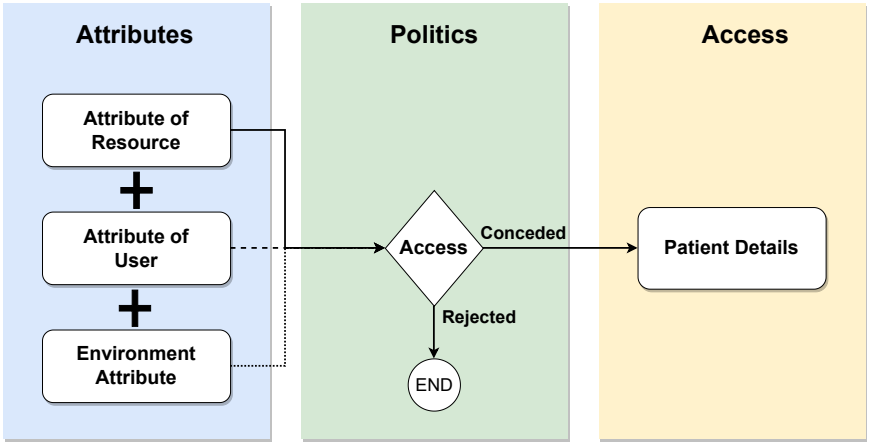

Figure 10. ABAC model.

Purpose-based access control (PBAC) aims to relate data to specific purposes. This mechanism uses roles and attributes to exploit ABAC and RBAC features. The central idea of this model is to grant access through the prior understanding in which data can be collected or accessed. The purposes are organized hierarchically through generalization and specialization principles [42]. This fact can contribute significantly to the privacy of sensitive data, although management may induce greater complexity depending on the control of each purpose.

The XACML standard defines five main components that deal with access decisions: policy administration point (PAP), policy enforcement point (PEP), policy decision point (PDP), policy information point (PIP), and context handler (CH). PAP stores and manages a persistent set of policies associated with destination identifiers. The PEP constitutes integrating any system in which the resources to be protected are stored and managed. The PEP receives access requests and blocks the flow of execution until a decision is made. At the same time, the PEP propagates the requests to the PDP, which is the main decision-making place for the incoming access request. The PDP retrieves all necessary attributes and contextual information from the PIP, evaluates the defined policies, and decides according to these policies. PIP is responsible for retrieving and storing attribute values. The context handler (CH) is responsible for deriving the context of a given request.

Figure 11 displays the various interactions between the components of the XACML standard, highlighting the chronological sequence of message exchanges during the access request process. Prior to an access request, it is necessary that (1) the PAP write policies and policy sets and make them available to the PDP. The access requestor (2) sends an access request to the PEP, which may include subject, resource, and environment attribute values. Subject attributes concern the patient in an emergency condition. The PEP then (3) constructs a standard XACML request context and sends it to the PDP, which (4) requests any additional subject, resource, and environment attribute values from the PIP. The PIP obtains the requested attributes and (5) returns them to the PDP. In turn, the PDP (6) asks the PAP for policies according to the purpose of the request. The PAP (7) returns the request policies for the PDP to (8) evaluate the related policy and returns the default XACML response context to the PEP. Finally, the PEP (9) executes the authorization decision, allowing or denying access.

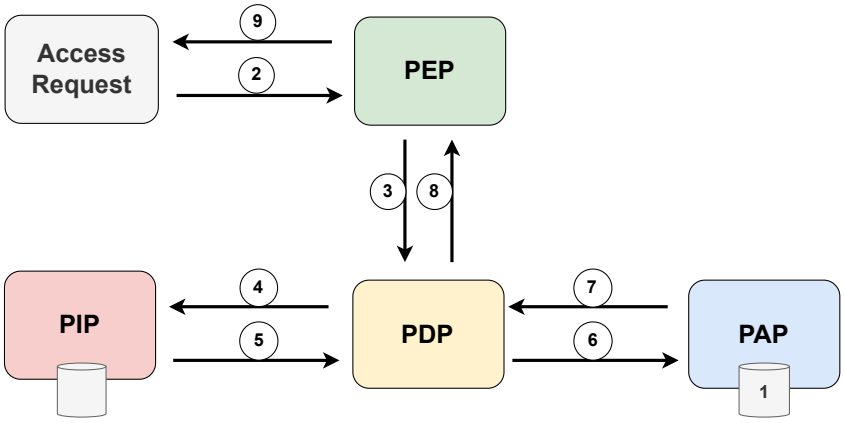

Figure 11. Architecture and flowchart of the XACML standard.

4.2. Data Protection Standards and Legislation

The increasing stringency of private data protection policies has led to limitations on centralized data processing approaches. The General Data Protection Regulation (GDPR) (available at https://gdpr-info.eu/ (accessed on 24 September 2023)) is a prominent law that establishes guidelines for processing the personal data of individuals within the European Union. To comply with the GDPR, organizations must undertake the crucial process of identifying sensitive data within their data repositories. This process involves various steps, including discovering and categorizing personal data based on their nature

and sensitivity, followed by implementing appropriate measures to safeguard the identified sensitive data. Specific privacy requirements, such as encryption and security protocols, need to be adhered to, especially when dealing with special categories of data like racial and health data, which require a valid and lawful basis for collection, storage, transmission, or processing [43].

Electronic medical records face particular challenges under the GDPR, as patient consent is crucial for data manipulation. The seventh article of the GDPR outlines the fundamental requirements for consent, and data controllers must demonstrate that data subjects have willingly consented to processing their data. Additionally, in cases where a contract or service provision depends on consent, data subjects must grant consent for processing personal data that is not essential for contract performance. Traditional methods of obtaining consent involve complex printed or digital documents, which pose logistical and security concerns. In this context, distributed smart contracts offer a fundamental solution for a fully digital world, streamlining the process of obtaining and managing consent securely and efficiently. Distributed smart contracts can facilitate compliance with the GDPR's consent requirements and ensure transparent data handling practices [43].

In Brazil's scenario, the General Data Protection Law (*Lei Geral de Proteção de Dados*—LGPD) is a federal law enacted in 2018 responsible for data protection throughout the national territory. Like the GDPR, the LGPD applies to any organization that processes personal data in Brazil, regardless of whether it is headquartered in the national territory. The law defines personal data as any information relating to a natural person or legal entity governed by public or private law. Personal information means name, address, e-mail, telephone number, identification number, and IP address, among others. The law identifies processing agents as the natural or legal person of public or private law that performs any processing operation on someone else's data. Among the duties established for these agents are the collection of explicit consent from the data subject and the provision of reports that identify the processing operations applied to the data, including the specification of its storage location, data masking, and protection measures. Several organizations must implement technical and organizational measures to guarantee the security and confidentiality of personal data. They also must report any data breaches to the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados*—ANPD) and affected individuals. The ANPD is responsible for policing compliance with the LGPD, imposing fines and penalties.

Under the LGPD, health data are classified as sensitive personal data, and their processing is subject to specific regulations. Like the General Data Protection Regulation (GDPR), the processing of sensitive data necessitates obtaining explicit consent from the data subject or their legal guardian, clearly highlighting the specific purposes for which the data will be used (available at https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (accessed on 24 September 2023)). An essential document commonly used for this purpose is the free and informed consent form (*Termo de Consentimento Livre e Esclarecido*—TCLE). The patient or their legal representative signs this document and aims to provide comprehensive information about potential risks, complications, or other relevant details related to a particular medical treatment or procedure. As it contains sensitive information, the data within this document are also governed by the LGPD. Despite ongoing digitization efforts, the manual filling and signing of TCLEs pose challenges in efficiently managing and securing the contained information.

- **Understanding of patients:** Patients have the right to understand the procedures for the storage, use, and retention of their health information by health professionals;
- **Confidentiality:** Health data are protected during storage and transmission using techniques such as encryption and authentication. Under no circumstance must the patient's health data be disclosed to third parties without prior authorization;
- **Patient control:** Patients must have the ability to control and authorize who can access and use their health data;

- **Data integrity:** Electronic patient health information must be protected from unauthorized modification or destruction;
- **Exception of consent:** In exceptional situations where a patient's life is at risk or in other critical circumstances, health information may be disclosed and used without the individual patient's consent;
- **Non-repudiation:** To ensure that responsible authorities fulfill their obligations about patient information, any relevant activities must be supported by verifiable evidence;
- **Auditing:** Regular monitoring of patient's health information and comprehensive recording of related activities are necessary to ensure data security. Patients must be provided with assurances regarding the security and protection of their health information.

The fundamental goal of the Health Insurance Portability and Accountability Act (HIPAA) is to safeguard individuals' health information, ensuring the proper flow of relevant data for healthcare provision and promotion. This regulation strikes a delicate balance between facilitating the use of essential health information and protecting the privacy of those seeking medical care (available at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (accessed on 24 September 2023)). The United States' diverse and extensive healthcare landscape necessitated a flexible and comprehensive approach, enabling HIPAA to encompass various uses and disclosures requiring attention. A critical facet of HIPAA pertains to its handling of health information breaches. The regulation defines a breach as the unauthorized use or disclosure of protected health information that compromises the security or privacy of such data under the "privacy rule". This rule sets stringent standards for safeguarding individuals' medical records and other personally identifiable health information. It mandates proper data protection measures to ensure sensitive data privacy while entitling individuals to examine and obtain copies of their health records. In case of a breach, it is presumed to be a violation unless the covered entity (insurance plans, hospitals, and clinics) or business associate can demonstrate a low probability of compromising the confidentiality of health information based on a risk assessment.

Certain exceptions are outlined in the definition of a violation. The first exception involves unintentional acquisition, access, or use of protected health information by a workforce member or someone acting under the authority of a covered entity or business associate, as long as it is conducted in good faith and within the scope of their authority. The second exception refers to the inadvertent disclosure of protected health information by an authorized individual at a covered entity or business associate to another authorized person within the organization. In both cases, the information cannot be further used or disclosed without proper authorization governed by the "privacy rule". The third exception encompasses situations where a covered entity or business associate possesses a good faith belief that the unauthorized recipient of the disclosure would not retain the information (available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (accessed on 24 September 2023)).

5. Solutions for Secure Integration and Sharing of Health Data

The integration and secure sharing of health data are critical issues for the evolution of health systems. The advancement of technology and the digitization of medical records give rise to several challenges related to interoperability and the protection of patient privacy. Patient data are spread across different data silos that do not communicate and do not necessarily use the same representation and communication standard, which makes it difficult to exchange information efficiently and securely. Even if it is possible to exchange information, sharing sensitive information requires robust protection measures, such as encryption and access control, to ensure that only authorized persons have access to the data and that the integrity of these data is preserved. Thus, the lack of standardization, the diversity of systems, data security, and regulatory issues make integration and secure sharing complex in healthcare. Several solutions have been developed to address these

issues, to improve the quality of care, facilitate the exchange of information between professionals, and ensure the security of sensitive data. In this context, we explore some of the solutions available on the market and proposals in the literature to promote the integration and secure sharing of health data.

5.1. Traditional Approaches

Traditionally, data security in healthcare facilities has been ensured through restricted access systems, protected by *firewalls*, with strict regulations regarding the breadth and amount of patient data that can be archived. More recently, cryptographic protocols have been applied.

The electronic system e-SUS (available at https://sisaps.saude.gov.br/esus/ (accessed on 24 September 2023)) brings together several tools aimed at reformulating primary care (*Atenção Básica*—AB) in order to computerize the SUS. e-SUS comprises two complementary software systems capable of instrumentalizing the medical data collection process. The Citizen's Electronic Record (*Prontuário Eletrônico do Cidadão*—PEC) focuses on the storage of all clinical and administrative information of the patient in the context of the UBSs, that is, any health establishment classified as a health post, basic health center, mixed units, or family health support center. The Simplified Data Collection (*Coleta de Dados Simplificada*—CDS) software is dedicated exclusively to structuring the registration and service forms, being specially adapted for scenarios without computerization or with limited, unstable, or non-existent connectivity. For this purpose, data insertion in the CDS can be carried out offline and later consolidated through a PEC with connectivity. The simplicity of the CDS entails a limitation in the local storage capacity of the embedded database and makes management functions unfeasible.

Regardless of the collection software used, the data are forwarded to the Health Information System for Primary Care (*Sistema de Informação em Saúde para a Atenção Básica*—SISAB), responsible for the national centralization of processing and disseminating data and information related to AB. Before being made available in the system, the data sent are submitted to a validation process to verify the originality, the fulfillment of temporal criteria, and the link with an establishment registered in the National Register of Health Establishments (*Cadastro Nacional de Estabelecimentos de Saúde*—CNES). Based on the consolidated data, SISAB issues performance reports containing health indicators by state, municipality, health region, and team. Access control to resources within e-SUS is based on access profiles, or roles, in which each profile is associated with a set of system resources that can be active or inactive, depending on the activities performed by the professional. Integration with third-party systems is made possible through the Apache Thrift API or by adopting standardized files in XML format. Thus, the existing system in a health unit must be able to generate Thrift /XML files, which are imported into the municipal PEC. PEC can generate reports of inconsistencies and control data transmission to SISAB through a national centralized system. Both alternatives, Thrift or XML, guarantee the interoperability of e-SUS APS with systems already implemented in municipalities, allowing the import of collected data and consolidation in SISAB.

The AGHUx platform (*Aplicativo de Gestão para Hospitais Universitários*—AGHUx) (available at https://www.gov.br/ebserh/pt-br/hospitais-universitarios/regiao-centro-oeste/hujm-ufmt/governanca/aghu (accessed on 24 September 2023)) focuses on the management of university hospitals and helps to standardize care and administrative practices at these hospitals. The Brazilian Company of Hospital Services (*Empresa Brasileira de Serviços Hospitalares*—EBSERH) develops the system and provides unified access to all electronic health records generated by the hospitals in the network. This integration provides a cross-sectional view of the patient's clinical trajectory, improving the continuity of treatments and care regardless of the hospital of origin. Remote access to medical information recorded in AGHUx is made possible through HU Digital (available at https://hudigital.ebserh.gov.br/ (accessed on 24 September 2023)), a digital platform available both in web format and through applications on mobile devices. HU Digital offers different interfaces depending

on whether the user profile accessing it is a healthcare professional or a patient. Patients can access their own data histories and enjoy digital services, such as issuing certificates and teleconsultations. Access permission from the web can be granted to individuals or specific teaching hospitals. Likewise, duly authorized doctors and nurses can authenticate themselves in HU Digital in order to consult discharge summaries, procedures, and surgeries performed or scheduled.

Figure 12 highlights the modules that makeup AGHUx. The modules are dedicated to administrative functions and medical procedures. The patients module handles the registration of patients in the system, subsidizing other care activities. Depending on the procedure performed at the hospital, the medical record can be opened. Through the on-line medical records (POL) module, all the patient's clinical information is viewed, including their history of records of care provided. The administrative ambulatory module is used in situations requiring simple procedures such as dressings, minor surgeries, and first aid. The ambulatory assistance module allows the physician to analyze care evolution within the office. The hospitalization module supports the management of hospital admissions, with features for admission, bed management, allocation of responsible professionals, discharge summary issues, and medical and administrative discharge. The nursing prescription module helps define the care applied to each patient based on the data collected and analyzed and the diagnosis established by the nursing team. The patient control module aims to computerize patient control records, covering monitoring processes and water control, allowing agility in viewing information and greater security in patient care. The medical prescription module registers diagnoses and medical prescriptions, generating behaviors and activities for the care team. The exams module consolidates diagnostic and therapeutic support services (SADT) records into an organized set of elements, including requests, follow-up, and results. The pharmacy module comprises the drug management process, including regulation, sorting, and dispensing activities. Closely linked to the previous one, the inventory module focuses on managing the movement of supplies by controlling the flow of materials, providing an efficient response to material requests. The surgery module details any actions related to complex surgical procedures, such as procedure description, room scheduling, usage time measurement, and cost calculation. Due to the system's modularity, the main challenge AGHUx faces is the mismatch between the system versions implemented in university hospitals and the implementation of modules, which may not be compatible with the existing system version in the hospital.

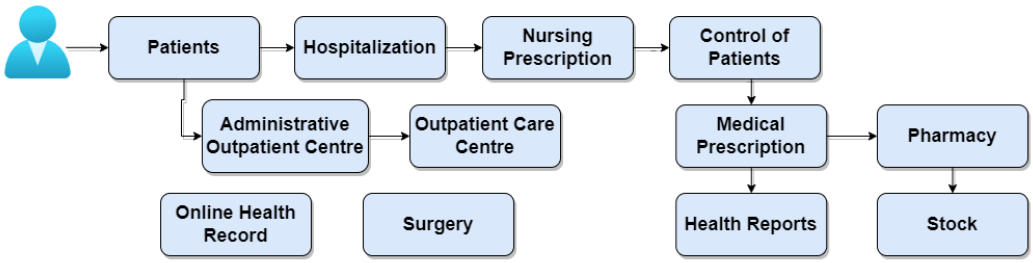

Figure 12. Overview of the AGHUx system's modules and the interaction between these modules.

Some commercially available solutions focus on specific areas of health, such as iDoc (available at https://idoc.radiomemory.com.br/ (accessed on 24 September 2023)), created for dental radiology. iDoc is a platform for online distributing exams and diagnoses, which gathers patient data and exams sent by different radiology clinics. Thus, iDoc centralizes patient information, allowing the dentist access to patient data even if the exams were performed in different clinics. The dentist can also add information about the patient, including history and history. The platform dispenses with printed exams, allowing the online sharing of digital exams stored in the cloud. iDoc can host digital files in formats such as JPEG, DICOM, STL, PLY, PPTZ, DOCX, and PDF (available at https://blog.radiomemory.com.br/conheca-o-idoc-academico/ (accessed on 24 September

2023)). The platform has the advantage of the speed and agility with which the exam is available for consultation. Once the exam is complete, the clinic can send it to the dentist. The platform also offers a variety of features, such as a digital model tool capable of analyzing the patient's dental arch in a three-dimensional format. There is no information available on how data access control is carried out.

Another commercial system is Alert (available at https://www.alert-online.com/br/ (accessed on 24 September 2023)), adapted for web and cloud. Alert is intended for the complete management of the electronic clinical process through various products that make up the solution. It includes several functionalities for monitoring the history of each patient, scheduling and alerting appointments or medical procedures, assigning discharges, issuing reports, teleservice, and order management. In addition, the software has an internal planning and business intelligence system. The solution uses interoperability standards, IHE, HL7, ITIL support, and international terminologies such as SNOMED, ICD, and LOINC. Access to the various products is achieved through a single-sign-on (SSO) mechanism that provides users with a centralized authentication scheme across the entire Alert application domain. SSO supports the integration of Alert products with LDAP or AD domains. Access to patient data is based on predefined profiles associated with each professional registered in the system.

GestãoDS (available at https://www.gestaods.com.br/ (accessed on 24 September 2023)) is medical software with online scheduling, financial control, telemedicine, medical marketing, and other features created to facilitate the management of clinics and offices. The software also provides digital signatures and ensures data privacy when processing, maintaining, and storing health-related information in compliance with HIPAA. The solution provides several access permission levels, separated into user profiles. In addition, it offers customized models of medical records and prescriptions according to the professional's standard of care.

5.2. Blockchain-Based Approaches

Incorporating blockchain technology in several applications has mainly been motivated by the possibility of generating irrefutable computational evidence, stored in a distributed manner, of the chronological order of transactions carried out. These benefits are desirable in EMR sharing solutions, as the traceability of accessed data is needed. In this sense, several blockchain-based solutions are proposed in the literature, some commercially available. Within the commercial scope, the Medicalchain (available at https://medicalchain.com/en/ (accessed on 24 September 2023)) platform, it is constituted as a health data market accessed by MedTokens. Five hundred million MedTokens were issued and sold in 2018. In this solution, the patient controls physicians' access to records, for example, during a telemedicine consultation, and can grant researchers access to records in exchange for MedTokens. MedTokens can also pay for medical appointments [44]. The solution is built on top of two blockchains and does not store medical data in the blocks. The first controls access to EMRs and is implemented using the Hyperledger Fabric platform. The second chain is used for generating the tokens, which is performed through the Ethereum Request for Comments 20 (ERC20) (pattern of *fungible token*) from Ethereum. A smart contract controls token distribution. Thus, Ethereum is used for payments.

Similar to Medicalchain, the MedChain solution uses two distinct token types: external tokens, called MedCoins, to provide access control and privacy; and internal tokens, called record tokens, to provide a map of the distributed patient record by adding cryptographic digests to the blockchain [45]. The blockchain platform used is Ethereum for verification anchoring and Hyperledger Fabric. MedChain records can include health data in various formats, such as plain text, digital images, or database objects. This information is stored in a distributed file system based on the InterPlanetary File System (IPFS). The address of a patient's record stored in the file system is associated with that patient's "patient block" on Ethereum. To retrieve all patient records, interact with a smart contract to obtain all addresses of all patient records. After getting the addresses, they can be used to request each

record from IPFS. Other solutions, like MediBChain, provide privacy [46] and protect the patient's identity using pseudonymity through cryptographic public keys. The proposal implements a permissioned blockchain-based patient-centric health data management system. There is no information about the platform used.

Among the academic solutions, the AuditChain proposal provides multilevel access control for patients, doctors, nurses, and hospital administrators for managing EMRs [47]. The proposal implements smart contracts using the Hyperledger Fabric platform [48,49]. The digital signature of the transaction uses public-key cryptography and serves as a virtual token for access control. The Medblock proposal [50] implements a data-sharing structure with an access control mechanism based on a signature scheme. Sensitive data and pointers to the patient's EMR are encrypted with a multi-signature scheme within the blockchain. The access control engine cycles through the blocks until it finds the correct block by comparing the signature with the collection of signatures in the ledger. The block's permission to see the encrypted content depends on the comparison result. Zhang et al. propose the FHIRChain for data sharing between physicians and researchers based on the FHIR standard [51]. FHIRChain meets five key interoperability requirements: user identification and authentication, secure data exchange, authorized data access, consistent data formats, and system modularity. Data access control is based on a smart contract that outputs an access token and runs on the Ethereum platform. Access tokens are defined for each data transaction, which uses asymmetric cryptography to protect off-chain data pointers. The proposal uses the users' digital health identities to encrypt the content so that only users with the correct digital identity private keys can decrypt the content. Dagher et al. propose Ancile, an Ethereum-based blockchain for a records management system that utilizes smart contracts for tighter access control and data obfuscation [52]. Ancile maintains patients' medical records in providers' existing databases, and the referral addresses to these records and their permissions for each record are stored in the smart contract. Ancile is designed to store the Ethereum addresses of all nodes that can interact with a registry, an access level, and a symmetric key encrypted with each node's public key. In contrast, Oliveira et al. developed an EMR distribution approach whose access control is patient-centered [53]. The approach relies on a public-key infrastructure (PKI) and blockchain technology. The idea is to inherit the trust in authenticity provided by the PKI and the integrity and accountability provided by the blockchain. The proposal is a distributed EMR with computationally simple infrastructure, refined access control, and low overhead.

Rouhani et al. propose an ABAC system for sharing EMR data [54], while Maesa et al. propose an ABAC system using the Ethereum blockchain platform [55]. By choosing to store attribute values in the blockchain, the values cannot be changed due to the property of immutability. On the other hand, the values are auditable, since their updates can only be performed through transactions and thus registered in the blockchain. However, both proposals do not consider that the attributes must be authenticated by the data processor organizations whenever they interact with the access control system. As an asynchronous system, the blockchain requires organizations to continually update the attributes of their professionals on the blockchain, a fact that burdens the dynamic attributes of health professionals. On the other hand, Ghorbel et al. propose keeping user attributes off-chain and relying on trusted authorities to maintain a list of users associated with their verified attributes [56]. Employing a smart contract, these authorities authenticate user attributes when requesting user data. The authors use the Quorum platform, which implements a permissioned version of the Ethereum blockchain. Internally, the Quorum platform adopts a flexible consensus mechanism, capable of supporting RAFT consensus for crash fault tolerance and variations in PBFT for Byzantine fault tolerance.

By associating blockchain technology and a signature scheme based on attributes over multiple authorities, Guo et al. propose a distributed EMR system [57] that allows the patient to manage personal health records (PHRs) safely. However, this facility also comes at a performance cost as it creates overhead to sign the transaction by multiple authorities.

The proposal also suffers from confidentiality issues concerning the data stored on the blockchain. Similarly, Dang et al. analyze the use of fog computing to store and protect EMRs and use attribute-based signatures to ensure EMR privacy and confidentiality in fog and cloud environments [58]. In turn, Yue et al. focus on providing fine-grained privacy control [33]. The proposed system uses mobile phones to interact with an access control gateway that controls block access on the blockchain. However, the gateway does not track transactions. Daraghmi et al. propose an incentive-based consensus mechanism that leverages the degree of reputation of healthcare providers concerning their efforts in maintaining medical records and creating new blocks in the blockchain [59]. The access control contract includes all the information related to specific permissions for each smart contract based record. The proposal lists the Ethereum blockchain addresses for all users with access permissions to the registry. The contract specifies the access level and symmetric key encrypted with each user's public key.

In Brazil, there is a notorious government solution for sharing health data on a national network, the National Health Data Network (*Rede Nacional de Dados em Saúde*—RNDS) (available at https://www.gov.br/saude/pt-br/assuntos/rnds (accessed on 24 September 2023)). RNDS is an integration platform developed by DataSUS and the Executive Secretariat of the Ministry of Health. When fully consolidated, the RDNS intends to include a digital repository of retrospective, concurrent, and prospective patient information. Its use will allow numerous establishments to share cross-sectional information on citizen service in an integrated, continuous, efficient, and quality manner. To simplify the interoperability of citizen medical records, the RNDS makes the patient's medical record history available in a blockchain structure shared between states. The platform architecture is shown in Figure 13. The platform has an infrastructure hosted in the cloud with dedicated containers distributed to the federated states. Each container is subdivided into informational and technological services, classified according to type, for example, minimal data set or related to security, and according to the degree of maturity of service development, as available or planned [60].

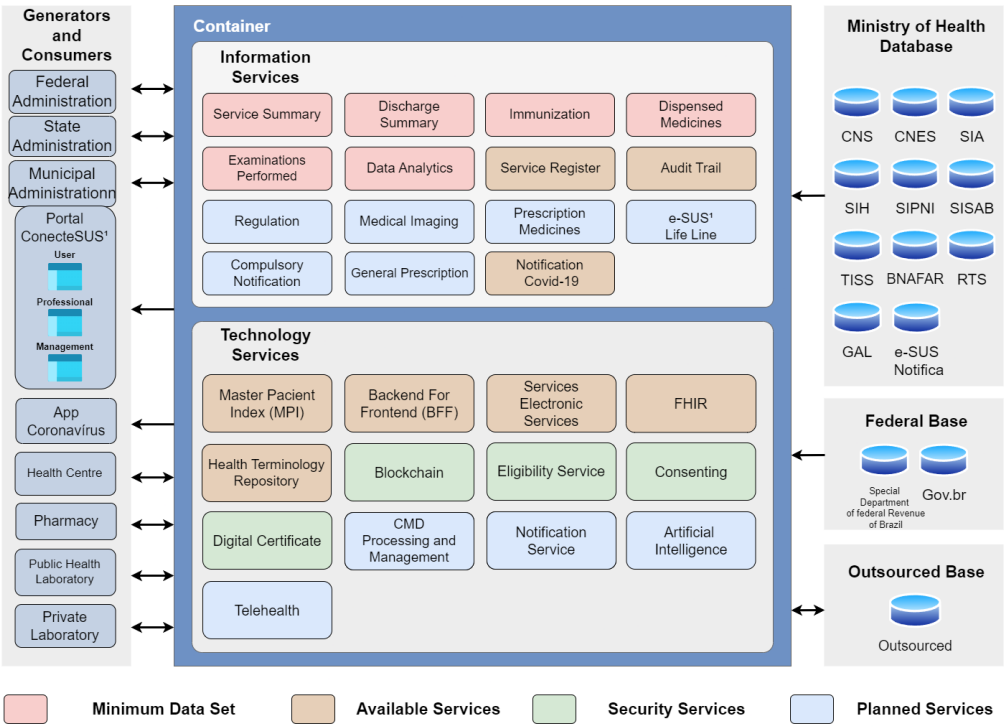

Figure 13. The RDNS architecture.

The technological services available include the Master Patient Index (MPI), a database that unifies the information of each patient registered by a health organization. Being a software design pattern, the backend for frontend (BFF) is responsible for delivering how information will be stored and consulted, regardless of the specificities of each type of graphical interface, for example, application and web portal. Electronic health services (EHR-services) focus RESTful services on exchanging information between digital health applications, especially PEC, portals, and web applications. The FHIR standard assists in exchanging health information between different establishments and institutions. The Repository of Terminologies in Health is a national virtual environment that houses classifications, nomenclatures, terminologies, taxonomies, information models, and standard definitions necessary for the standardization of semantic resources and information models to be used in the health sector [60].

Among the technological security services, the most relevant is related to blockchain technology. The RNDS provides for implementing a private and permissioned blockchain based on Hyperledger Fabric and running the Raft consensus mechanism [61]. Each container represents a blockchain node and will be located in a healthcare facility. The adoption of the blockchain aims to store the history of interactions between patients and health professionals, in addition to containing references to electronic health records. Currently, the RNDS blockchain has only one node, which does not guarantee the characteristic properties of the technology. The recovery process of any patient's health data via blockchain needs to satisfy some premises: (i) the access request must originate from an appropriate software tool, and (ii) the applicant must be part of an establishment registered with the CNES and have the correct credentials. If a professional requests access to any document or patient's medical record, it is only attended to with the patient's consent and explicit authorization in emergency medical circumstances or when the "opt-out" strategy is configured in the context of care at the health facility. The "opt-out" strategy assumes in advance that the patient authorizes the flexibility of the rules for accessing their data. Thus, if the patient wishes to change the permission policy, they may do so upon request [61]. Internally, the metadata are used in the ledger and distributed among the various network participants. Clinical documents will be used in private data collection, a native feature of Hyperledger Fabric, allowing a subset of organizations to endorse, confirm, or query private data without creating a separate channel. This feature ensures document storage privacy and economy. Since the documents will only be stored in the custodial organization and a limited structure of backup organizations, there will not be eventual excessive storage of the clinical documents. As shared in the ledger, the patient's history will be accessible to any organization, facilitating patient queries in healthcare facilities. Interoperability between systems is ensured by adopting the FHIR standard and LOINC terminology for data traffic and storage. Initially, the RNDS foresees transition microservices capable of converting data sent in CDA, OpenEHR, and FHIR. In order to avoid incomplete or printed medical records, the platform intends to implement smart contracts written in the GO language. The smart contract inclusion ensures that the business rules involved in electronic medical records are effectively complied with [61].

The RNDS complements the security added to the system by the blockchain, offering services such as (i) issuance of digital certificates, that is, electronic documents containing data about the individual or legal entity that uses it, serving as a virtual identity that confers legal validity and aspects of digital security; (ii) eligibility service, a service validating the available data that defines whether or not the health professional is qualified to access the citizen's data, applying rules for linking the professional with the health establishment, professional category, installation certification, and electronic medical record; (iii) consent, related to the opt-out consent model. By default, implicit consent is assumed until the citizen chooses to explicitly revoke consent [60].

Preliminary evaluations using the architectural proof of concept estimate that the RNDS will be able to support up to 1800 transactions per second (tps), a satisfactory rate to support the annual number of services provided for in the SUS [61]. Currently, the

Ministry of Health provides three portals to access the information stored in the RNDS, the ConectaSUS Cidadão, ConectaSUS Profissional, and ConectaSUS Gestão, aimed at patients, health professionals, and managers. By accessing the portal, citizens obtain vaccination history and other personal health records, health professionals view the entire clinical trajectory and patients' procedures, and managers can monitor the evolution of health indicators, which is fundamental for coordinating public policies. Table 3 summarizes the main features presented by healthcare solutions based on blockchains.

Table 3. Characteristics related to blockchain-based healthcare solutions.

		MediBChain [46]	MedicalChain [44]	MedChain [45]	Patel et al. [62]	Ghorbel et al. [56]	AuditChain [47]	FHIRChain [51]	MedRec [63]	Medblock [50]	Ancile [52]	RNDS †
Type	**Characteristics**											
Blockchain	Private Permissioned										✓	✓
	Public Permissioned	✓				✓		✓		✓		
	Private Not Permitted				✓							
	Not Specified		✓[1]	✓[1]			✓[1]		✓[1]			
Consensus Mechanism	Proof of Work	✓						✓	✓		✓	
	Prof of Participation				✓							
	Consensus Raft											✓
	Practical Byzantine Fault Tolerance		✓	✓								
	Consensus Hybrid or Proprietary									✓		
	Not Specified					✓[2]	✓[2]					

† Available at https://www.gov.br/saude/pt-br/assuntos/rnds (accessed on 24 September 2023). ✓[1]: The authors only report that the blockchain is permissioned, not specifying it as public or private. However, it is assumed to be a private network. ✓[2]: The authors only report that the consensus mechanism adopted is flexible.

6. Discussion, Trends, and Research Challenges

While potentially usable, blockchain technology is still considered complementary to legacy systems and does not replace them. Table 4 summarizes the main technical obstacles to incorporating blockchain technology in healthcare. Scalability is a potential obstacle to the conventional adoption of blockchains in the health sector. While not impactful on private blockchains, lack of scalability is an issue of concern on public blockchains. Compared to traditional transaction networks, capable of processing thousands of transactions per second, public blockchains are limited to tens of transactions per second [64,65]. Depending on the platform and consensus mechanism implemented, the latency introduced by the block validation process can reach up to 10 min [64]. Furthermore, an inappropriate consensus choice impacts increasing block creation time. At the same time, as the number of transactions and nodes in the network increases, more checks must be performed and, consequently, the greater the probability of bottlenecks. From the health systems perspective, these potential delays adversely affect the analysis of tests and the rapid definition of diagnoses [66]. However, there is a plurality of approaches capable of resolving this issue. One of the approaches is sharding, a technique based on dividing the network into different fragments (*shards*) so that the compulsory duplication of communication, data storage, and computational overhead is avoided for each participating node. This approach relieves each node of dealing with the entire transactional load of the network, allowing it only to maintain data about its fragment [67]. Another approach is to modify the traditional linear structure of blockchains to a representation in the form of a directed acyclic graph (DAG). In this new structure, each transaction is linked to multiple transactions, allowing the validation process to be parallel [68].

Blockchain-based healthcare systems are developed by grouping multidisciplinary concepts encompassing information technology knowledge, skills, and care flow in the medical field. However, the low presence of qualified professionals and the high com-

plexity of handling and maintenance contribute to such systems being frequently linked to poor usability [66]. In 2019, the Regional Center for Studies for the Development of the Information Society (*Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação*—Cetic.br) pointed out that only 20% of health establishments, whether private or public, had a professional with health training allocated in their respective departments from you. The percentage presence of internal IT teams in health establishments also accompanies this shortage of health professionals working in the technical area shortage in the Brazilian scenario. Around 21% of healthcare facilities have an internal team dedicated to technical support in the IT area, while 39% have a service provider hired by the facilities. Difficulties are reduced by prioritizing the creation of intuitive and user-enabled interfaces.

Table 4. Challenges faced in the use of blockchain technology in healthcare systems.

Technical Obstacle	Challenges
Scalability	Block size and block creation time
	Adoption of inefficient consensus mechanisms
	Higher confirmation times for creating a block
	Exponential increase in the number of checks as the number of transactions and nodes in the network grows
Usability	Complexity in developing and maintaining blockchain-based health systems
	Lack of professionals familiar with managing complex peer-to-peer networks
Irreversibility	Immutability of information stored in blocks
Privacy and Security	Using conventional digital signatures is vulnerable to quantum computing
	Majority percentage of network computing power is controlled by a single entity
Interoperability	Use of different consensus mechanisms, transaction mechanisms and smart contract functionalities

Intrinsic to blockchains, the immutability characteristic establishes that the stored data cannot be changed after being registered in blocks. As each node in the network has a replica of the chain, any attempt to modify data in one of these replicas is translated by the participating nodes as an imminent attack. Therefore, these alteration attempts are rejected, making it impossible to erase or edit the data, which cannot be performed by the authors or by court order [20]. This feature imposes on blockchain-based systems the need to deal with the irreversibility of records made on the chain. While authenticity is tamper-proof on a blockchain, there are no guarantees about the accuracy of stored data. Thus, blocks containing false or incorrect information cannot be removed or modified, even if intentionally inserted. The inflexibility in handling data contrasts with the storage needs present in EMR systems. Some data are temporarily stored because they do not present critical or valuable attributes for future diagnoses. Other data, such as the address or personal characteristics of patients, although not critical, require constant updates. Both situations highlight that the indiscriminate data storage in the blockchain is a limiting factor for adopting the technology, given the impossibility of deleting old records. Another challenging factor is the exposure of private keys. If this happens, patient data will be exposed to any individuals or entities holding the private key, with no possibility of using a new key to re-encrypt the data already registered in the chain. Therefore, any key leak permanently exposes the patient's privacy if their data are recorded in jail [65].

Another sensitive aspect is data privacy and security since all nodes access data transmitted by another node. When accessing their own information or medical history, patients are dependent on an intermediary entity in the event of an emergency. This factor breaches the privacy principles established in current data protection legislation. The expansion of the computational power of modern systems poses severe threats to blockchain security, especially when they are based on public-key cryptography. This vulnerability is related to the assumption that classical computers cannot decompose large numbers quickly. However, this hypothesis is refuted by the emergence of quantum computing, an emerging

technology that intends to solve highly complex cryptographic challenges quickly and efficiently. Among the alternatives to face this challenge, the replacement of conventional digital signatures by quantum-resistant cryptography [69] stands out. At the same time, PoW-based networks are also prone to breaching cryptographic security. This violation occurs through the 51% Attack, a malicious action in which a group of miners owns the majority fraction of the computational power of the blockchain network and, therefore, these nodes dictate the process of adding blocks to the network [20]. Therefore, a health system damaged by this attack can mean the loss of credibility for organizations.

Addressing the challenges related to interoperability is essential to harness the potential of blockchain technology in healthcare. Interoperability refers to the ability to exchange information between systems with heterogeneous characteristics. Achieving interoperability between the two EMR systems requires that the broadcast messages be based on standardized encoded data. While the absence of blockchain standards simplifies the role of developers, this vagueness contributes to communication problems between disparate systems. Thus, several blockchain networks based on different consensus mechanisms, transaction mechanisms, and smart contract functionalities exacerbated the lack of interoperability between systems. In healthcare, the adoption of traditionally disparate clinical technologies, technical specifications, and functional capabilities also impedes creation and sharing of data in a single format. Even when developed on the same platform, different EMR systems are not interoperable, since they were designed to meet a health institution's specific needs and preferences. In practice, the lack of standardized data limits the sharing of data electronically for patient care. A plausible solution to this problem is the development of new standards that can be adhered to by legacy solutions. For that purpose, the Enterprise Ethereum Alliance (available at https://entethalliance.org/ (accessed on 24 September 2023)) (EEA) introduced a standardized version of the Ethereum blockchain [20,69].

In addition to the technical challenges related to blockchain adoption, healthcare systems have several challenges. The interoperability challenges between systems, standardization, data integration, data security, and privacy stand out. Interoperability between systems is vital for quick and easy access to accurate and up-to-date patient information to make informed clinical decisions. However, health data management and interoperability between systems are challenging due to the heterogeneity of information and systems. The various systems must be developed considering good information security practices. Health data must be standardized for consistency and interoperability across disparate systems. Standards also govern the capture, storage, and retrieval of information. Thus, the developed systems must comply with the internationally adopted standards, and there should be regular backups and clear data retention policies to prevent loss. Compliance with standards also ensures the quality of captured data. Additionally, it should be possible to conduct regular audits of the data to improve the reliability of the information. Data integration systems can also help connect different health systems and databases, allowing data to be shared securely and efficiently. APIs can standardize how different systems and databases communicate and interact, allowing information and data to be shared more easily and securely. Some ongoing research projects and government actions in the area of health systems integration are:

- Common Platform (available at https://cordis.europa.eu/project/id/225005 (accessed on 24 September 2023)) is a research project funded by the European Union that aims to develop a common platform for sharing health information between different European countries. The project uses communication and security standards to ensure that health data are shared securely and efficiently;
- Integrating Data for Analysis, Anonymization, and SHaring (iDASH) [70] is a research project funded by the US government that aims to develop a platform for sharing health data between different health organizations. The project employs anonymization and security techniques to ensure that health data are shared safely and securely;

- RNDS is a Brazilian government initiative that develops a national interoperability platform for exchanging health data. The main objective is to facilitate access and exchange of data between the different public and private health information systems in Brazil. The platform enables the secure exchange of health data in a standardized manner and compliance with current privacy and security policies.

Health data security in traditional healthcare systems constitutes a paramount concern, necessitating robust measures to safeguard patient privacy and control data access. These measures encompass the implementation of information security policies, encryption of sensitive data, user authentication, and continuous monitoring to detect and thwart suspicious activities. Integrating various tools into medical routines stimulates discussions surrounding data management and security practices within the healthcare domain, underscoring the demand for user-friendly, cost-effective, and agile software with solid security practices [71]. The medical environment is characterized by intricate and dynamic characteristics involving complex procedures, routine changes, and the constant evolution of health-oriented technologies. Consequently, manipulating healthcare data by geographically dispersed medical teams increases data flows and imposes robust security measures, including encryption, to ensure data confidentiality. Moreover, as the volume of digital health data expands, there is a heightened risk of malicious actors seeking unauthorized access to this valuable information. Organizations must establish effective data management practices to address these challenges, ensuring compliance with regulatory requirements and relevant standards. Defining roles and responsibilities is crucial to ensuring that only authorized personnel access sensitive data securely. Additionally, introducing digital health systems adds complexity to the hospital environment, necessitating comprehensive training for multidisciplinary teams to guarantee safe and continuous access to sensitive data [72].

The COVID-19 pandemic has catalyzed a rapid surge in the integration of technologies within the healthcare sector. Past disease outbreaks have already underscored the risk of overwhelming healthcare facilities. The WHO responded to the pandemic by updating operational planning guidelines, seeking to strike a balance between addressing COVID-19 directly and ensuring the continuity of existing health services while upholding the standard of health and hygiene necessary to tackle endemic and future health challenges. Consequently, the demand for programs that foster quality communication, assistance, and care has intensified, prompting the urgent need for development. However, this urgency has given rise to several issues, such as non-communicative software solutions during medical consultations conducted via the Internet, thereby complicating medical assistance due to the proliferation of disparate systems. In such a scenario, achieving interoperability becomes crucial for effective patient care. Numerous works and experimental studies have explored the rapid evolution of telehealth, leading to many new challenges while reigniting previously known ones. Therefore, the critical attributes of interoperability, transparency, security, speed, and availability are vital considerations for driving future advancements and innovations in telehealth. Consequently, the trajectory of health research is heavily focused on telehealth and the development of innovative systems to address the current healthcare landscape.

Telehealth is a strategically significant area of healthcare, driven by its inherent potential for innovation, cross-disciplinary integration of technological advancements, and dynamic interconnections with various domains (available at https://www.who.int/fr/news/item/30-03-2020-who-releases-guidelines-to-help-countries-maintain-essential-health-services-during-the-covid-19-pandemic (accessed on 24 September 2023)). The growing prevalence of chronic diseases, including heart failure, lung disease, and diabetes, which can be effectively monitored through telehealth, further underscores its importance. By facilitating improved access to healthcare services, cost reduction, enhanced patient outcomes, and reduced transmission of infectious diseases through fewer in-person healthcare visits, telehealth has become a valuable tool in the healthcare landscape. The European Union's efforts to standardize and implement telehealth exemplify its recognition of its potential im-

pact (available at https://dialnet.unirioja.es/servlet/articulo?codigo=5635387 (accessed on 24 September 2023)).

Interoperability plays a pivotal role in the success of telehealth, as it allows seamless and secure sharing of patient information among healthcare providers, minimizing errors and enhancing patient care. Advancements in technologies such as robotization and automation in central laboratories, alongside the proliferation of new devices for peripheral and personal use, are bolstered by interoperability. Standards governing interoperability enable the development of decentralized systems, fostering efficient communication among diverse components. Brazil's Ministry of Health has taken proactive measures to foster telehealth by establishing interoperability standards through Ordinance No. 2073 of 2011, reflecting the nation's commitment to integrated and effective healthcare systems. The continued development and standardization of telehealth promise to revolutionize healthcare delivery and enhance patient outcomes worldwide.

Another challenge relates to the privacy of health data. The internet of things paradigm, which disseminates and popularizes the use of everyday objects such as cameras and mobile and wearable devices capable of communicating with each other, allows the monitoring of patient's health. In China, for example, a system that remotely determined who should quarantine during the COVID-19 pandemic used data obtained through thermal cameras in public places with facial recognition technology and an app that checked the vital functions of users daily. Several European countries used mobile networks to inform and identify people at risk of contamination [73]. These applications raise concerns related to the privacy of users and the management of these users' data. It is speculated that portable and wearable devices will continue to grow, with them increasingly used in digital health care [73]. Therefore, it is essential to seek solutions that protect users' privacy.

7. Conclusions

The rapid evolution of information and communication technology (ICT) tools in the healthcare sector highlights the increasingly vital role of electronic systems and digital platforms. The ability to efficiently and accurately share patient information across different medical systems can revolutionize healthcare delivery, improve patient care, and drive innovative research. However, the challenge lies in the inherent complexity and diversity of data formats used in various medical systems, making interoperability difficult and crucial to achieving these transformative goals. As a result, the complexity of the medical system prevents easy access to a patient's complete medical history when needed, leading to the loss or repetitive collection of information, making diagnosis and treatment challenging and negatively impacting the patient's journey.

EMRs are pivotal in facilitating access to distributed data, enabling standardized retrieval of patient information, and promoting care integration across healthcare teams and various medical facilities. However, sharing sensitive patient data without appropriate consent remains a significant concern, raising questions about data privacy and security in such healthcare systems. The ongoing COVID-19 pandemic has emphasized the urgent need to streamline care and exchange information between patients, physicians, and healthcare institutions. Patient records have gained even more importance in public health decision making, as data on diagnoses and prescribed medications can be instrumental in identifying individuals at risk of diseases like COVID-19. Moreover, the greater availability of patient data in electronic formats holds immense value in decision-making processes and ensuring continuity of care across both public and private healthcare sectors, encouraging information exchange between these spheres. The early detection of disease outbreaks is paramount in efficiently coordinating public health policies and prevention strategies at the national level.

Despite the potential transformative impact of electronic healthcare systems, challenges persist. Most EMR systems are built on centralized client–server architectures, posing concerns regarding data privacy and security vulnerabilities. Such vulnerabilities can lead to system failures and open opportunities for cyber attackers to compromise

patient data. Additionally, patient records are often fragmented across local databases, making it challenging to consolidate a comprehensive electronic medical history for each patient. Standardization of data formats becomes a critical requirement for achieving interoperability in the healthcare industry. Establishing a common language for exchanging and interpreting medical data would enable seamless communication between different systems, fostering greater collaboration and data sharing.

Blockchain technology is a potential solution for standardizing and facilitating interoperation between health systems. However, integrating blockchain into healthcare systems comes with its technical challenges. Among the key concerns surrounding blockchain adoption in healthcare are scalability, usability, immutability, privacy, security, and interoperability. Scalability becomes a potential obstacle in the widespread adoption of public blockchains, as they may face limitations in transaction processing speed and block validation time, potentially impacting medical examination analysis and timely diagnosis. Usability is another crucial challenge, as managing and maintaining complex blockchain-based systems, combined with a shortage of qualified professionals with expertise in health and ICT, often leads to systems with low usability.

The immutability feature in blockchain poses unique challenges concerning data manipulation, as once data are written to a block, it cannot be modified or deleted. This characteristic can be problematic for storing non-critical or temporary data. Additionally, the transparency of blockchain networks and the reliance on intermediaries to access personal health information can compromise patient privacy and confidentiality. Achieving robust data privacy and security in blockchain-based healthcare systems remains a key concern.

Interoperability is essential to successfully exchanging information between heterogeneous systems within the healthcare industry. The lack of standardization and multiple blockchain networks with different consensus mechanisms, transaction methods, and smart contract functionalities hinder interoperability efforts. Addressing these technical challenges is essential to leverage the full potential of blockchain technology and foster collaboration and innovation in the healthcare sector.

In the digital health market, there is a growing awareness of the importance of interoperability between health information systems, as data security and access to comprehensive patient information are crucial aspects of providing quality care. Current limitations in interoperability also hinder effective integration between records scattered across various clinics and hospitals, underscoring the urgency of addressing these issues. Developing research projects and commercial products that focus on standardization and integration in electronic medical record-sharing systems becomes crucial to realizing the transformative possibilities in healthcare, promoting positive patient outcomes, and shaping a future characterized by collaboration and innovation in the medical domain. Given the evidence and arguments discussed externally in this article, we emphasize that our conclusions are consistent and directly address the main challenges and potential solutions related to the interoperability of electronic health systems, with a particular focus on the role of blockchain technology.

Author Contributions: Conceptualization, D.M.F.M., D.S.V.M. and M.T.d.O.; methodology, D.M.F.M. and D.S.V.M.; validation, D.M.F.M., D.S.V.M. and N.R.d.O.; investigation, D.M.F.M. and D.S.V.M.; resources, D.M.F.M. and D.S.V.M.; writing—original draft preparation, A.C.R.M. and N.R.d.O.; writing—review and editing, D.M.F.M., D.S.V.M., N.R.d.O., A.C.R.M., R.V., Y.d.R.d.S., G.N.N.B. and M.T.d.O.; visualization, N.R.d.O.; supervision, R.V., D.M.F.M. and D.S.V.M.; project administration, D.M.F.M. and D.S.V.M.; funding acquisition, D.M.F.M. and D.S.V.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by CNPq, CAPES, RNP, FAPERJ, FAPESP (2018/23062-5) e Niterói City Hall/FEC/UFF (Edital PDPA 2020).

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

References

1. Makary, M.A.; Daniel, M. Medical error—The third leading cause of death in the US. *BMJ* **2016**, *353*, i2139. [CrossRef] [PubMed]
2. Dubovitskaya, A.; Xu, Z.; Ryu, S.; Schumacher, M.; Wang, F. Secure and trustable electronic medical records sharing using blockchain. In *AMIA Annual Symposium Proceedings*; American Medical Informatics Association: Bethesda, MD, USA, 2017; Volume 2017, p. 650.
3. Stoeger, K.; Schmidhuber, M. The use of data from electronic health records in times of a pandemic—A legal and ethical assessment. *J. Law Biosci.* **2020**, *7*, lsaa041. [CrossRef] [PubMed]
4. Hurst, W.; Tekinerdogan, B.; Alskaif, T.; Boddy, A.; Shone, N. Securing electronic health records against insider-threats: A supervised machine learning approach. *Smart Health* **2022**, *26*, 100354. [CrossRef]
5. Cetic.br. *Pesquisa Sobre o uso das Tecnologias de Informação e Comunicação nos Estabelecimentos de Saúde Brasileiros: TIC Saúde 2019*; Núcleo de Informação e Coordenação do Ponto BR (NIC.br): Sao Paulo, Brazil, 2020.
6. Janett, R.S.; Yeracaris, P.P. Electronic Medical Records in the American Health System: Challenges and lessons learned. *Cienc. Saude Coletiva* **2020**, *25*, 1293–1304. [CrossRef]
7. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [CrossRef]
8. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 1–3. [CrossRef]
9. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
10. Engelhardt, M.A. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technol. Innov. Manag. Rev.* **2017**, *7*, 22–34. [CrossRef]
11. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
12. Namasudra, S.; Sharma, P.; Crespo, R.G.; Shanmuganathan, V. Blockchain-based medical certificate generation and verification for IoT-based healthcare systems. *IEEE Consum. Electron. Mag.* **2022**, *12*, 83–93. [CrossRef]
13. Health Level Seven International. *HL7 Implementation Guide for CDA® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm) Draft Standard for Trial Use Release 2.1*; Technical Report; Health Level Seven International: Ann Arbor, MI, USA, 2015.
14. DICOM Standards Committee. DICOM PS3.1 2023b. Technical Report; 2023. Available online: https://dicom.nema.org/medical/dicom/2023b/output/pdf/part01_changes.pdf (accessed on 24 September 2023).
15. Savage, R. *HL7 Version 2.5.1, Implementation Guide for Immunization Messaging*; Technical Report; Centers for Disease Control and Prevention: Atlanta, GA, USA, 2014.
16. Maani, R.; Camorlinga, S.; Arnason, N. A Parallel Method to Improve Medical Image Transmission. *J. Digit. Imaging* **2011**, *25*, 101–109. [CrossRef]
17. Massad, E.; Marin, H.d.F.; Azevedo Neto, R.S.d. (Eds.) *O Prontuário Eletrônico do Paciente na Assistência, Informação e Conhecimento Médico*; USP: São Paulo, Brazil, 2003.
18. Harrison, J.E.; Weber, S.; Jakob, R.; Chute, C.G. ICD-11: An international classification of diseases for the twenty-first century. *BMC Med. Inform. Decis. Mak.* **2021**, *21*, 206. [CrossRef] [PubMed]
19. World Health Organization. *International Classification of Diseases, Eleventh Revision ICD-11*; Technical Report; World Health Organization: Geneva, Switzerland, 2022.
20. Mattos, D.M.; Medeiros, D.S.; Fernandes, N.C.; de Oliveira, M.T.; Carrara, G.R.; Soares, A.A.; Magalhães, L.C.S.; Passos, D.; Carrano, R.C.; Moraes, I.M.; et al. Blockchain para Segurança em Redes Elétricas Inteligentes: Aplicações, Tendências e Desafios. *Sociedade Brasileira de Computação*. 2018. Available online: https://research.tudelft.nl/en/publications/blockchain-para-seguran%C3%A7a-em-redes-el%C3%A9tricas-inteligentes-aplica%C3%A7 (accessed on 24 September 2023).
21. Xu, X.; Weber, I.; Staples, M.; Zhu, L.; Bosch, J.; Bass, L.; Pautasso, C.; Rimba, P. A taxonomy of blockchain-based systems for architecture design. In Proceedings of the 2017 IEEE international conference on software architecture (ICSA), Gothenburg, Sweden, 3–7 April 2017; pp. 243–252. [CrossRef]
22. Pustokhin, D.A.; Pustokhina, I.V.; Shankar, K. Challenges and Future Work Directions in Healthcare Data Management Using Blockchain Technology. In *Applications of Blockchain in Healthcare*; Springer: Singapore, 2021; pp. 253–267. [CrossRef]
23. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 24 September 2023).
24. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]
25. Cachin, C.; Vukolic, M. Blockchain Consensus Protocols in the Wild (Keynote Talk). In Proceedings of the 31st International Symposium on Distributed Computing (DISC 2017), Vienna, Austria, 16–20 October 2017; Richa, A.W., Ed.; Dagstuhl, Germany, 2017; Volume 91, pp. 1:1–1:16. [CrossRef]
26. Carrara, G.R.; Burle, L.M.; Medeiros, D.S.V.; de Albuquerque, C.V.N.; Mattos, D.M.F. Consistency, availability, and partition tolerance in blockchain: A survey on the consensus mechanism over peer-to-peer networking. *Ann. Telecommun.* **2020**, *75*, 163–174. [CrossRef]

27. Luh, F.; Yen, Y. Cybersecurity in Science and Medicine: Threats and Challenges. *Trends Biotechnol.* **2020**, *38*, 825–828. [CrossRef]
28. Rahman, A.; Hossain, M.S.; Alrajeh, N.A.; Alsolami, F. Adversarial Examples—Security Threats to COVID-19 Deep Learning Systems in Medical IoT Devices. *IEEE Internet Things J.* **2021**, *8*, 9603–9610. [CrossRef]
29. Salim, M.M.; Park, J.H. Federated Learning-Based Secure Electronic Health Record Sharing Scheme in Medical Informatics. *IEEE J. Biomed. Health Inform.* **2023**, *27*, 617–624. [CrossRef]
30. Lesk, M. Electronic medical records: Confidentiality, care, and epidemiology. *IEEE Secur. Priv.* **2013**, *11*, 19–24. [CrossRef]
31. Tormo, G.D.; Mármol, F.G.; Girao, J.; Pérez, G.M. Identity management–in privacy we trust: Bridging the trust gap in ehealth environments. *IEEE Secur. Priv.* **2013**, *11*, 34–41. [CrossRef]
32. Zhang, X.; Poslad, S. Blockchain support for flexible queries with granular access control to electronic medical records EMR. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6. [CrossRef]
33. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef]
34. Jacquemard, T.; Doherty, C.P.; Fitzsimons, M.B. Examination and diagnosis of electronic patient records and their associated ethics: A scoping literature review. *BMC Med. Ethics* **2020**, *21*, 76. [CrossRef]
35. Haas, S.; Wohlgemuth, S.; Echizen, I.; Sonehara, N.; Müller, G. Aspects of privacy for electronic health records. *Int. J. Med. Inform.* **2011**, *80*, e26–e31. [CrossRef] [PubMed]
36. de Oliveira, M.T.; Verginadis, Y.; Reis, L.H.; Psarra, E.; Patiniotakis, I.; Olabarriaga, S.D. AC-ABAC: Attribute-based access control for electronic medical records during acute care. *Expert Syst. Appl.* **2023**, *213*, 119271. [CrossRef]
37. Nazerian, F.; Motameni, H.; Nematzadeh, H. Emergency role-based access control E-RBAC and analysis of model specifications with alloy. *J. Inf. Secur. Appl.* **2019**, *45*, 131–142. [CrossRef]
38. Seol, K.; Kim, Y.G.; Lee, E.; Seo, Y.D.; Baik, D.K. Privacy-Preserving Attribute-Based Access Control Model for XML-Based Electronic Health Record System. *IEEE Access* **2018**, *6*, 9114–9128. [CrossRef]
39. Peleg, M.; Beimel, D.; Dori, D.; Denekamp, Y. Situation-based access control: Privacy management via modeling of patient data access scenarios. *J. Biomed. Inform.* **2008**, *41*, 1028–1040. [CrossRef] [PubMed]
40. Abomhara, M.; Yang, H.; Køien, G.M. Access control model for cooperative healthcare environments: Modeling and verification. In Proceedings of the 2016 IEEE International Conference on Healthcare Informatics (ICHI), Chicago, IL, USA, 4–7 October 2016; pp. 46–54. [CrossRef]
41. Abomhara, M.; Ben Lazrag, M. UML/OCL-based modeling of work-based access control policies for collaborative healthcare systems. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 1–6. [CrossRef]
42. Byun, J.W.; Bertino, E.; Li, N. Purpose Based Access Control of Complex Data for Privacy Protection. In Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies, New York, NY, USA, 8–10 June 2005; SACMAT '05; pp. 102–110. [CrossRef]
43. Larrucea, X.; Moffie, M.; Asaf, S.; Santamaria, I. Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0. *Comput. Stand. Interfaces* **2020**, *69*, 103408. [CrossRef]
44. Albeyatt, A. MedicalChain White Paper 2.1. Technical Report, MedChain White Paper 2.1, 2018.
45. Sandgaard, J.; Wishstar, S. MedChain White Paper 2.1. Technical report, MedChain White Paper 2.1, 2018. Available online: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf (accessed on 24 September 2023).
46. Al Omar, A.; Rahman, M.S.; Basu, A.; Kiyomoto, S. MediBChain: A blockchain based privacy preserving platform for healthcare data. In Proceedings of the Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, 12–15 December 2017; Proceedings 10; Springer: Berlin/Heidelberg, Germany, 2017; pp. 534–543. [CrossRef]
47. Anderson, J. Securing, Standardizing, and Simplifying Electronic Health Record Audit Logs through Permissioned Blockchain Technology. *Unthrr*, 2018. Available online: https://digitalcommons.dartmouth.edu/senior_theses/135/ (accessed on 24 September 2023).
48. Rebello, G.; Camilo, G.; Silva, L.; Souza, L.; Guimarães, L.; Alchieri, E.; Greve, F.; Duarte, O. Correntes de Blocos: Algoritmos de Consenso e Implementação na Plataforma Hyperledger Fabric. *Sociedade Brasileira de Computação*, 2019. Available online: https://dl.acm.org/doi/abs/10.1145/3544538.3544653 (accessed on 24 September 2023).
49. Agrawal, D.; Minocha, S.; Namasudra, S.; Gandomi, A.H. A robust drug recall supply chain management system using hyperledger blockchain ecosystem. *Comput. Biol. Med.* **2022**, *140*, 105100. [CrossRef]
50. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. MedBlock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, *42*, 136. [CrossRef]
51. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying blockchain to securely and scalably share clinical data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [CrossRef]
52. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]

53. de Oliveira, M.T.; Reis, L.H.; Carrano, R.C.; Seixas, F.L.; Saade, D.C.; Albuquerque, C.V.; Fernandes, N.C.; Olabarriaga, S.D.; Medeiros, D.S.; Mattos, D.M. Towards a blockchain-based secure electronic medical record for healthcare applications. In Proceedings of the ICC 2019-2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6. [CrossRef]
54. Rouhani, S.; Belchior, R.; Cruz, R.S.; Deters, R. Distributed attribute-based access control system using permissioned blockchain. *World Wide Web* **2021**, *24*, 1617–1644. [CrossRef]
55. Maesa, D.D.F.; Mori, P.; Ricci, L. A blockchain based approach for the definition of auditable access control systems. *Comput. Secur.* **2019**, *84*, 93–119. [CrossRef]
56. Ghorbel, A.; Ghorbel, M.; Jmaiel, M. Accountable privacy preserving attribute-based access control for cloud services enforced using blockchain. *Int. J. Inf. Secur.* **2021**, *21*, 489–508. [CrossRef]
57. Guo, R.; Shi, H.; Zhao, Q.; Zheng, D. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access* **2018**, *6*, 11676–11686. [CrossRef]
58. Dang, L.; Dong, M.; Ota, K.; Wu, J.; Li, J.; Li, G. Resource-efficient secure data sharing for information centric e-health system using fog computing. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6. [CrossRef]
59. Daraghmi, E.Y.; Daraghmi, Y.A.; Yuan, S.M. MedChain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access* **2019**, *7*, 164595–164613. [CrossRef]
60. Santos, S.d.L.V.d.; Zara, A.L.d.S.A.; Lucena, F.N.d.; Ribeiro-Rotta, R.F.; Braga, R.D.; Amaral, R.G.; Pedrosa, S.M.; Kudo, T.N. *Rede Nacional de Dados em Saúde: O que Precisamos Saber*?; Cegraf UFG: Goiânia, Brazil, 2022.
61. Tribunal de Contas da União (TCU). *Levantamento de Aplicações Blockchain: Aplicações Blockchain no Setor Pública do Brasil (Apêndice 1)*; Sumário executivo; Tribunal de Contas da União (TCU): Brasília, Brazil, 2020.
62. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2019**, *25*, 1398–1411. [CrossRef]
63. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [CrossRef]
64. Chowdhury, M.J.M.; Ferdous, M.S.; Biswas, K.; Chowdhury, N.; Kayes, A.; Alazab, M.; Watters, P. A comparative analysis of distributed ledger technology platforms. *IEEE Access* **2019**, *7*, 167930–167943. [CrossRef]
65. Lo, S.K.; Xu, X.; Chiam, Y.K.; Lu, Q. Evaluating suitability of applying blockchain. In Proceedings of the 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS), Fukuoka, Japan, 5–8 November 2017; pp. 158–161.
66. De Aguiar, E.J.; Faiçal, B.S.; Krishnamachari, B.; Ueyama, J. A Survey of Blockchain-Based Strategies for Healthcare. *ACM Comput. Surv.* **2020**, *53*, 27. [CrossRef]
67. Yu, G.; Wang, X.; Yu, K.; Ni, W.; Zhang, J.A.; Liu, R.P. Survey: Sharding in blockchains. *IEEE Access* **2020**, *8*, 14155–14181. [CrossRef]
68. Kaur, G.; Gandhi, C. Scalability in blockchain: Challenges and solutions. In *Handbook of Research on Blockchain Technology*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 373–406. [CrossRef]
69. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations. *Neural Comput. Appl.* **2022**, *34*, 11475–11490. [CrossRef]
70. Ohno-Machado, L.; Bafna, V.; Boxwala, A.A.; Chapman, B.E.; Chapman, W.W.; Chaudhuri, K.; Day, M.E.; Farcas, C.; Heintzman, N.D.; Jiang, X.; et al. iDASH: Integrating data for analysis, anonymization, and sharing. *J. Am. Med. Inform. Assoc.* **2011**, *19*, 196–201. [CrossRef] [PubMed]
71. Araujo Gomes de Castro, F.; Oliveira dos Santos, Á.; Valadares Labanca Reis, G.; Brandão Viveiros, L.; Hespanhol Torres, M.; de Oliveira Junior, P.P. Telemedicina rural e COVID-19: Ampliando o acesso onde a distância já era regra. *Revista Brasileira Medicina Família Comunidade* **2020**, *15*, 2484. [CrossRef]
72. Blandford, A.; Wesson, J.; Amalberti, R.; AlHazme, R.; Allwihan, R. Opportunities and challenges for telehealth within, and beyond, a pandemic. *Lancet Glob. Health* **2020**, *8*, e1364–e1365. [CrossRef]
73. Chén, O.Y.; Roberts, B. Personalized Health Care and Public Health in the Digital Age. *Front. Digit. Health* **2021**, *3*, 595704. [CrossRef]