Management Issues in Healthcare System

2025(11)1–16

EUROKD

EPR Governance Based on Architectural Techniques and Blockchain and Smart Contracts Technologies

Andreia de Castro Costa Xavier*, Claudio Gottschalg-Duque, Tomás Roberto Cotta Orlandi

Universidade de Brasília-UNB, Brasília-Brazil

Received *18 November 2024* ***Accepted*** *11 February 2025*

ABSTRACT

This study proposes an archival management method for Electronic Health Records (EHRs) based on architectural techniques and Blockchain and Smart Contracts technologies to ensure governance, security, and privacy in Health 4.0 contexts. Given the increasing relevance of EHRs as sources of information, evidence, and research in digital healthcare ecosystems, the research highlights challenges related to data governance, interoperability, and cybersecurity. Through a qualitative, exploratory approach, the authors present a method structured in seven macro-processes, covering the EHR lifecycle from capture to permanent archival or disposal. The implementation of private Blockchain networks and Smart Contracts automates processes, guarantees data integrity, and strengthens patients' control over their personal data, aligned with legal frameworks for data protection. The findings reinforce the need for innovative archival practices and technological strategies to enhance efficiency, security, and transparency in healthcare information management.

Keywords: *Electronic Health Records, Document Management, Blockchain, Smart Contracts, Health 4.0, Data Governance, Interoperability.*

How to cite this article:

Xavier, A. D C. C., Gottschalg-Duque, C., & Orlandi, T. R. C. (2025). EPR Governance based on architectural techniques and blockchain and smart contracts technologies. *Management Issues in Healthcare System*,*11*,1-16. https://doi.org/10.32038/mihs.2025.11.01

Corresponding author's E-mail address: andreiaccx@gmail.com

Studies point to a future in which software with artificial intelligence will be able to measure data, perform diagnoses, and indicate the need for medical treatments, raising the standard in the provision of medical services, whose main beneficiary will be the patient. As a result, the role of the Electronic Patient Record (EPR) becomes more relevant as a source of evidence, information, research, and interoperability of personal data in the area of Health 4.0, related to the use of advanced technologies and technological trends such as robotics, artificial intelligence, cybernetics, the Internet of Things, etc. (Nabeto, 2020). As a digital archival document, the EPR requires document management (DM) based on these technologies, particularly Blockchain (blockchain) and Smart Contracts (smart contracts), aiming at the governance, security, and protection of the privacy and personal data of its holders who are part of the Information Society (Castells, 2012): “The medical record is a valuable element for the patient and the institution that treats him/her, for the doctor, and for teaching, research and public health services, also serving as an instrument of legal defense” (Goes et al., 2013).

Digital transformations should allow greater integration between organizations and health service providers to enable the interoperability of the EHR in favor of streamlining its management and decision-making, as well as the evolution of the MyData concept (Poikola et al., 2020), to allow its holder to control and participate in decisions related to the processing of their data. However, there are some challenges from an archival point of view related to the governance of the EHR, such as the absence of a Document Management Program (DMP), the adoption of technical archival requirements in the computerized systems used, and reliable digital archival repositories (RDC-Arq) for its digital conservation and preservation. In the scope of information security and cybersecurity, the obstacles presented are personal data vulnerable to unauthorized access, tampering, kidnapping, and commercialization in the Dark Web market due to computerized EHR management systems susceptible to security breaches and cyberattacks. Therefore, it is necessary to curate EHRs to ensure legal compliance, operational efficiency, and the protection of your sensitive personal data, as they contain health-related information protected by access to information and personal data protection laws.

The combination of Blockchain and Smart Contracts technologies offers significant potential to increase security and automate transactions and processes, which can be especially valuable in the governance of EHRs. According to Duque and Lyra (2010, p. 42), governance involves the ability of managers to effectively implement principles, guidelines, and controls that ensure consistent and predictable fulfillment of an organization's social objectives and legal obligations.

Archival Document Management in the Context of Health

With the advancement of "Health 4.0", it is essential to integrate DM into your processes and products to optimize your results by providing complete and reliable data, since in the era of the big data phenomenon, access to quality information will be a competitive advantage as important as the benefits of artificial intelligence and robotics. Reliable data will provide greater credibility and assertiveness to medical history, diagnosis, prognosis and indication of medical treatments. Such data are especially contained in EHRs, considered repositories of primary sources, as they contain technical and administrative information for decision-making and for generating secondary sources of information, such as reports and statistics, which can contribute to public

policies and health campaigns. This DM is defined as "a set of procedures, routines, and activities related to the production, organization, use, archiving, and disposal of documents, which may result in their disposal for elimination or permanent storage, depending on their evidentiary or informational value. Elimination is independent of the support on which the document is registered, whether paper or digital" (CONARQ, 2020a).

DM, with a focus on EHRs, is necessary to support technological advances in healthcare due to the following facts:

- The archival document is testimonial, as it contains the record of medical actions and decisions requiring rigorous management to guarantee its integrity, reliability, accessibility, maintenance, and preservation throughout its life cycle so that it can serve as evidence of acts, facts, and events.
- Organizing documents facilitates access to health information and communication processes;
- Compliance with citizens' rights to health, as established in the Brazilian Federal Constitution, becomes faster and more assertive to benefit organizations and, especially, patients.

This DM, in turn, involves technical procedures, including the production, processing, use, evaluation, and archiving of documents in the current and intermediate phases, aiming at their elimination or collection for permanent storage, and aims to support decision-making, ensure compliance with duties, protect rights, provide access to information and promote transparency in administrative actions.

Electronic Health Record

The EHR is a fundamental component of healthcare and health records, as it contains information about the patient's physical and mental condition recorded by a multidisciplinary healthcare team and therefore serves to support the comprehensive and ongoing care of the patient, the activities of healthcare professionals and organizations, as well as research institutions. It has evolved over time and has a vast history of development and use. "A single document consisting of a set of information, signals, and recorded images generated from facts, events, and situations about the patient's health and the care provided to him/her of a legal, confidential, and scientific nature, which enables communication between members of the multidisciplinary team and the continuity of care provided to the individual" (DOU, 2002).

To contribute to EHR governance, it is necessary to implement DM in healthcare organizations, which will be detailed below.

Planning Archival Management

DM planning involves analyzing the institutional reality, establishing guidelines and procedures, designing the archival management system, and developing instruments and manuals. Through a diagnosis, it is possible to analyze basic information about documents and files, including quantity, location, physical condition, storage conditions, degree of growth, frequency of consultation, and other relevant information that will allow the development of an archival project defined as a

planning instrument that arises as a result of the diagnosed problems (Lopes, 2013). It details the activities, products, schedule, and steps to be developed for the implementation of DM.

The implementation of the project marks the beginning of document management activities or the implementation of a Document Management Program (DMP), which aims at economy, efficiency, effectiveness, and control of document production, including documents, such as EHRs, in the health area.

Document Archival Management Program Applied to EHR

The DMP includes executing actions and projects foreseen in the Archival Management Planning and comprises main and accessory work instruments, which will be detailed below.

Main:

- Document Classification Plan (DCP): is a logical scheme used to organize documents into classes, subclasses, groups, and subsets. It is based on the organization's activities, regardless of its medium (paper or digital). The DCP is essential for the effective organization and retrieval of documents.
- Document Temporality and Destination Table (DTDT): is an important tool that helps control retention periods and the destination of documents based on a classification plan. It defines how long documents should be kept in the current and intermediate phases and whether they should be eliminated or preserved permanently.
- Manual of Archival Document Management: includes procedures for the production, classification, processing, archiving, and destination of documents and may contain a glossary with conceptual definitions from the field of Archival Science, which can also be incorporated into the DCP and DTDT (CONARQ, 2020a) .

Accessories:

- Controlled vocabulary: consists of a set of standardized terms for indexing documents in computerized systems.
- Thesaurus: controlled list of terms related by semantic, hierarchical, association, or equivalence criteria (CONARQ, 2020a). Its main function is to organize and control the terms used to index and retrieve information.

It is also recommended to use a Computerized Document Archival Management System (CDAMS), based on the Requirements Model for Computerized Document Management Systems (e-ARQ Brazil), to integrate the DCP, and in the context of EHRs, the requirements of a CDAMS can be incorporated into a specialized system for managing these records. In addition to the CDAMS, it is suggested to adopt the Guidelines for implementing a Reliable Digital Archival Repository – RDC-Arq, in accordance with long-term preservation standards. Blockchain and Smart Contracts technologies are proposed to assist in the technological security and DM of EHRs.

Studies point to a future in which software with artificial intelligence will be able to measure data, perform diagnoses, and indicate the need for medical treatments, raising the standard in the provision of medical services, whose main beneficiary will be the patient. As a result, the role of the Electronic Patient Record (EPR) becomes more relevant as a source of evidence, information,

research, and interoperability of personal data in the area of Health 4.0, related to the use of advanced technologies and technological trends such as robotics, artificial intelligence, cybernetics, the Internet of Things, etc. (Berger et al., 2024; Nabeto, 2020; Tracy et al., 2024). As a digital archival document, the EPR requires document management (DM) based on these technologies, particularly Blockchain (blockchain) and Smart Contracts (smart contracts), aiming at the governance, security, and protection of the privacy and personal data of its holders who are part of the Information Society (Castells, 2012): "The medical record is a valuable element for the patient and the institution that treats him/her, for the doctor, and for teaching, research and public health services, also serving as an instrument of legal defense" (Goes et al., 2013).

Digital transformations should allow greater integration between organizations and health service providers to enable the interoperability of the EHR in favor of streamlining its management and decision-making, as well as the evolution of the MyData concept (Poikola et al., 2020), to allow its holder to control and participate in decisions related to the processing of their data. However, there are some challenges from an archival point of view related to the governance of the EHR, such as the absence of a Document Management Program (DMP), the adoption of technical archival requirements in the computerized systems used, and reliable digital archival repositories (RDC-Arq) for its digital conservation and preservation. In the scope of information security and cybersecurity, the obstacles presented are personal data vulnerable to unauthorized access, tampering, kidnapping, and commercialization in the Dark Web market due to computerized EHR management systems susceptible to security breaches and cyberattacks. Therefore, it is necessary to curate EHRs to ensure legal compliance, operational efficiency, and the protection of your sensitive personal data, as they contain health-related information protected by access to information and personal data protection laws.

Blockchain

Blockchain emerged as a technology designed for cryptocurrency transactions, such as Bitcoin. Due to its unique properties, its use has expanded across several domains, appearing as one of the key technologies for driving innovations in the area of Health 4.0, and is defined as: "Technology that allows the recording of transactions permanently, not allowing changes to previous transactions, only recordings of new transactions, thus maintaining a mathematically, practically, inviolable history in the current computational parameters. The participants of the negotiation and the object computationally guaranteed their inviolability. This set can be a contract, a commercial transaction, a civil registry, a real estate registry, agreements, or commitments; in short, any object whose validation and reliability are publicly and jointly verified and guaranteed, both by the actors and by the validators distributed in the world wide web" (Ferraz, 2019, p. 23).

This technology has fundamental characteristics such as the immutability and irreversibility of records, distributed databases, peer-to-peer transmission, and computational logic, contributing to expanding the digitalization of services with data security (Andrew et al., 2023; Pang et al., 2022).

How Blockchain Works

Blockchain's operation includes using hashes to control the content, chronological records (timestamps), digital signatures, and data authenticity verification through mining, which is described as a computational mathematical process (Rodrigues, 2017). This makes this technology one of the safest, allowing advances in data interoperability, easier access to information, and increased trust for those who use it.

Each blockchain block contains a hash generated based on the block's contents, including the data recorded. This hash serves as a unique "fingerprint" that identifies the block. When a new block is added to the blockchain, it contains the previous block's hash, thus creating a chain of interconnected blocks (Kumar et al., 2021). If a hacker tries to change any data in a previous block, it will affect the calculation of the hash for that block. As a result, the hash of that block would no longer match the one stored in the subsequent block. This would create a discrepancy that all nodes in the blockchain network would immediately detect. This is one of the reasons why blockchains are considered secure and immutable. Any attempt to tamper with previous data requires significant computing power, as the hacker would have to recalculate the hashes for all subsequent blocks. This makes this task extremely difficult and expensive, which, in practice, makes it almost impossible. Thus, Blockchain security is strongly based on encryption and the distributed nature of the network, which make transactions and records resistant to tampering and fraud.

Blockchains Types

Publics

The main features of public Blockchain are:

- Anyone can join the network, participate, edit, and validate new blocks;
- Activities and information are public and transparent, meaning anyone can see all transactions and records, and
- Actions are decentralized, and there is no central control.

Private (Permissioned):

The main features of Private Blockchain are:

- only authorized nodes (computers) can join the network and perform permitted actions. Participants are known and usually subject to approval;
- access control is strict, allowing stakeholders to define who can participate and what actions can be performed on the network;
- It is similar to a controlled corporate intranet, where companies have complete control over participants and operations, and
- offers greater privacy and control compared to public Blockchains.

Due to the need to protect personal data contained in EHRs, the recommended use is private or permissioned Blockchain networks, as they are restricted to a group of previously registered and

authorized people or organizations and contain rules and supervision regarding their operation. To support the use of the private Blockchain network by EPR management systems, it is suggested to use Smart Contracts.

Smart Contracts

Smart Contracts "are a form of automated digital contract, in which the terms of a transaction are embedded in a computer code, to be recognized by software when given a certain input" (Silva, 2020, p. 27). They contain algorithms capable of self-executing when predefined conditions are met. They are designed to automate various types of transactions and business processes and execute actions and contractual clauses based on specific events. Conceived by Nick Szabo in 1996, they gained prominence with the rise of Blockchain technology, especially Ethereum, as they are a significant innovation that takes advantage of the intrinsic properties of that technology while providing the flexibility necessary to optimize its use.

The main points of this technology are listed below:

- Benefits of Smart Contracts: These smart contracts have the potential to reduce costs, deadlines, and errors in execution, eliminate intermediaries by allowing agreements between unknown parties, and streamline processes, making them effective in areas such as payments, access control, records, and execution of contractual clauses.
- Decentralized execution: they run on a decentralized computer network that validates and executes the code. This decentralization ensures transparency, security, and immutability of a contract.
- Trustless transactions: operate in a "trustless" environment where participants do not need to trust each other or intermediaries. The code and Blockchain network ensure the automatic execution of the contract without third parties.
- Various applications: in addition to financial transactions, they can be used in various areas, such as supply chain management, decentralized applications, voting systems, insurance, etc.
- Application Example: A practical example of how Smart Contracts are used can be seen on the Airbnb platform, where the housing rental contract is executed automatically when the contractual conditions are met on the Blockchain network.
- Immutable and transparent: once on the Blockchain, Smart Contracts are immutable, meaning their code cannot be changed. The entire transaction history and contract execution are transparent and publicly accessible in the case of a public Blockchain network.
- Challenges and limitations: the use of Smart Contracts still faces challenges and limitations, such as security vulnerabilities, complexity in coding, and the need for greater regulation and development of artificial intelligence capabilities to deal with adverse events. In addition, collaboration between professionals from different areas is essential for their development.

Smart contracts have the potential to revolutionize various businesses, products, and services by automating and ensuring the security of contractual processes. However, their development and use require a solid understanding of Blockchain technology, programming, and specific use case requirements.

In the context of governance applied to EPRs, Smart Contracts are considered an important ally of Blockchain as they can assist in self-executing procedures related to EHRs, including those of DM.

Archival Management of EHRs associated with Blockchain and Smart Contracts Technologies

EHRs contain sensitive personal information, that is, information that may cause some type of prejudice to its holder and, in many cases, are accessible via the Internet. For this reason, they must be protected against cyberattacks and "unauthorized interventions that may result in the tampering or loss of documents" (CONARQ, 2020a). Blockchain technology is an attractive solution to guarantee the security of this data, and Smart Contracts are a differentiator by offering access control and permissions to EHRs, as well as the automation of processes and activities, such as auditing medical records.

The management of EHRs is complex and particularly relevant in a scenario where the privacy and security of patient data must be a priority, without neglecting the facilities that technology provides, such as data interoperability, to gain scalability in accessing and sharing information between service providers; optimization of time; rationalization of the use of financial, logistical, security and workforce resources; consolidation of information; reduction of errors in decision-making and greater independence for patients to control their own data.

EHR Data Interoperability

Interoperability refers to the ability of different healthcare systems and applications to communicate and share data effectively. In the context of medical records, interoperability is necessary to ensure that a patient's records are accessible to doctors, hospitals, and other healthcare providers, regardless of their geographic location or the system they are using.

Initiatives such as the data management model called MyData, by authors Poikola et al. (2021), can contribute to the interoperability of EHR data and put the individuals in control of their own data, allowing them to choose with whom they wish to share their information. In addition, it optimizes the use and promotes transparency and governance of data that different platforms and devices can access.

This model works as follows:

- Digital Account Holder: Each individual has a personal "digital account" that contains information about themselves.
- User Panel: The data subject has a "user panel" that serves as an interface to manage their information. Through this panel, the person can grant, modify, or revoke consent from third parties to use their data.
- Data Distribution: Unlike traditional models, where data is stored centrally, this model distributes data across multiple servers and applications. This helps protect data privacy, as it is not concentrated in a single location and is provided only to meet specific purposes.
- Data Sharing on Request: Data sharing only occurs when it is requested. This means that services that want to access a user's data need to obtain permission from the user through their control panel.

- Consent Management: Data subjects have full control over their consent. They can decide which services or applications can access their data and under what circumstances. This puts control over the use of personal data in the hands of individuals.
- Interoperability and Portability: One of the goals of MyData is to promote data interoperability and portability. This means that data can be used in multiple contexts, and data subjects can easily transfer it from one service to another.
- Security and Privacy: By distributing data and allowing data subjects to control consent, the MyData model seeks to ensure greater security and privacy of personal data.

Furthermore, to assist in the interoperability of EHRs, there are also studies on the Unique Patient Identifier (PII or UPID) designed to uniquely represent a patient in a hospital or health system (Mayer et al., 2020). It is used to uniquely distinguish each patient and ensure that their health information is traceable and associated with them accurately. A unique identifier is essential to avoid mismatches in medical records and to identify an EHR data subject unequivocally.

However, data interoperability in healthcare organizations is a significant challenge due to the diversity of standards, protocols, and information systems used and concerns about data security. This lack of interoperability can hinder healthcare efficiency and the sharing of information between healthcare institutions and represent an obstacle to improving patient care. To address this problem, there are several strategies, such as creating healthcare ecosystems based on technologies such as (private) Blockchain and Smart Contracts to improve the security and control of access to health data. This approach creates a safer environment for sharing sensitive patient information, minimizing risks and unauthorized access.

Furthermore, making information available in open standards is a key strategy for addressing interoperability challenges. Its use helps ensure that different healthcare systems can understand and process data in a consistent manner. This makes sharing information between healthcare organizations easier, even if they use different systems. It benefits healthcare professionals by enabling more efficient and secure access to medical records and promotes better quality of medical care for patients.

For the governance of EHRs, it is proposed that health organizations adopt the Document Management Maturity Level, which is measured by compliance with goals established by the National Archives.

Maturity Level in Document Management

The concept of "Maturity Level" refers to a measure that assesses the development and effectiveness of a given area or process in an organization. This term originated in the 1970s when Nolan proposed four stages of growth for the IT department. Over time, this approach has developed and is now used in several areas, including information management (Becker et al., 2009; Proença et al., 2018).

Maturity levels are usually structured hierarchically, indicating different stages of evolution in related practices and processes. In the context of document management, as exemplified by the National Archives, this term is used to assess the maturity of DM practices in institutions. Each maturity level is achieved based on specific criteria. Level 1 involves the existence of protocolizing

units and document control. Subsequent levels include the definition of DM policies, classification and organization of documents, internal rules for disposal, process mapping, digital preservation, and integration of archival systems. The benefits of the different levels include efficiency in public administration, transparency, accountability, support for political and administrative decisions, availability of information, economy, optimization of space use, and preservation of relevant documents.

The maturity levels in DM can be applied in healthcare settings and to EHRs with significant benefits for patients, professionals, and healthcare organizations regarding efficiency, transparency, and decision support. This includes implementing archival techniques to control information from creation to disposal or permanent storage.

Material and Method

To achieve the objectives of this research, it was necessary to adopt a scientific method containing criteria and strategies to collect relevant information, including bibliographic research and data collection activities. This helped to establish the basis for the subsequent stages of the research, including the analysis of the results and the proposal of the method for archival management of EHR, comprising Blockchain and Smart Contracts technologies. The main aspects of this scientific method are highlighted below:

- Research Classification: this research was classified based on its purpose, level, design, and nature and was considered applied, exploratory, bibliographic, and qualitative.
- Research Methodological Strategy: The strategy adopted for the research involved a systematic search of the literature on Blockchain, Smart Contracts, and topics related to Archiving and Electronic Health Records (EHR), in addition to identifying and selecting a process modeling notation.
- Research Methodological Path: the sequence of steps followed during the research went from choosing the topic to developing a method for EHR archival management using Blockchain and Smart Contracts technologies.
- Research Corpus: systematic literature searches were conducted in seven databases for scientific articles on the research topic.
- Narrative Review: Besides the systematic search, the research also used a narrative review to find articles associated with technical terms in Archival Science.
- To develop the EHR archival management method using Blockchain and Smart Contracts technologies proposed in the research, studies related to processes, business process management, and process modeling were necessary.

Method Proposed in the Research

The research achieved its objective through the method created for the archival management of EHRs using Blockchain and Smart Contracts, covering processes, subprocesses, and activities. Here are the main points covered in the method:

- The objective of the Method: The method aimed to create an effective process for managing EHRs, incorporating archival techniques and advanced technologies, such as Blockchain and Smart Contracts, containing as premises the DM, security, and protection of the privacy of

personal data contained in the EHRs, in accordance with the General Data Protection Law, and focusing on the holder of the EHR, who is the patient.

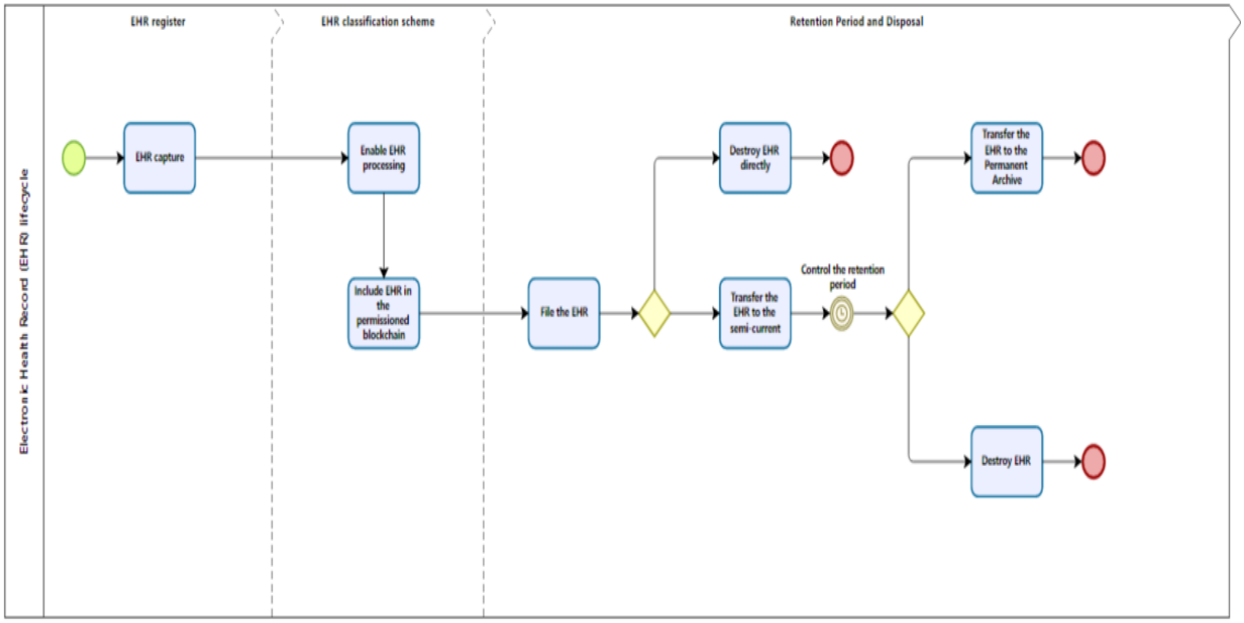
- Use of BPMN: To visually represent the method, we chose to use the BPMN (Business Process Modeling and Notation) notation, chosen for its ability to represent business processes at a high level and make the method more accessible to different audiences.
- Macro process Steps: The method was divided into seven main processes covering everything from the EHR capture to its disposal or collection for permanent storage. Each process is described below:

    Process 1: EHR Capture;
    Process 2: Access and Security Classification Scheme;
    Process 3: Include the EHR in a private (permissioned) Blockchain network;
    Process 4: Archive the EHR;
    Process 5: Delete the EHR;
    Process 6: Transfer the EHR to the Intermediate Archive;
    Process 7: Retrieve the EHR to the Permanent Archive.

The visual representation, together with the description of the EHR Life Cycle Method, are recorded in Figure 1 and Table 1:

Figure 1

Method: EHR life cycle



Note. Source: Xavier & Gottschalg-Duque (2021)

Table 1
Method Details: EHR Life Cycle

Method based on knowleDMe of Archival Science, considering the use of Blockchain and Smart Contracts technologies, for the management and privacy of the Electronic Patient Record (EHR)

Activities	Detailing
1 – EHR capture	Definition: Capture consists of declaring a document as an archival document, incorporating it into the DM system through registration, classification, indexing, assignment of metadata and restriction of access and archiving (CONARQ, 2020a).
2 – Enable EHR processing	Definition: Refers to the granting of permission for use, intervention and access to the EHR, including production, reading, updating and deletion of documents (CONARQ, 2020b)
3 – Including EHR in the Permissioned Blockchain	Definition: Refers to the procedure of including the EHR in the permissioned Blockchain network with control of use, intervention and access managed by Smart Contracts. Blockchain is a type of Distributed LeDMer Technology (DLT) whose translation is "Distributed LeDMer Technology" and whose operation resembles "a database distributed across several nodes or computing devices" (Gomes, 2018). Private Blockchain "arose from a demand for access control to activities carried out within the network. In this case, only authorized nodes can enter and perform permitted actions" (Cedro & Dos, 2020).
4 – Archive the EHR	Definition: means that the system will automatically store the digital file(s) in a storage device (physical operation) and record, in metadata, elements that establish the organic relationship between the documents (logical operation), such as, for example, document identifier, process/dossier number and classification code (CONARQ, 2020b).
5 – Eliminate EHR	Definition: "To eliminate means to destroy documents that, in the assessment, were considered to have no value for permanent storage" (CONARQ, 2020a).
6 – Transfer the EHR to the Intermediate Archive	Definition: "Transfer is the transfer of documents from the current archive to the intermediate archive, where they will await compliance with storage deadlines and final destination" (CONARQ, 2020b).
7 – Collect the EHR for Permanent Archive	"Collection is the entry of documents into permanent archives according to the archival jurisdiction to which they belong. The documents to be collected must be accompanied by instruments that allow their identification and control, in accordance with current legislation" (CONARQ, 2020b).

Note. Source: Xavier & Gottschalg-Duque (2021)

Results and Discussions

The systematic search of the literature and the analysis of scientific articles related to the research topic was fundamental to acquiring knowledge and insights and realizing the relevance of continuing to explore the application of emerging technologies in the area of Archival Science and health records, aiming to improve the management and security of documents, such as EHRs, and the protection of patient privacy.

As a result of this research, it was possible to make inquiries and proposals regarding relevant issues regarding the management of EHRs and the need to review the policies and retention periods for these documents, among them:

- Proposal for CCD and DTDT for the health sector: the possibility of developing a CCD and DTDT as a reference for the health sector, including EHRs, should be considered. These instruments can facilitate document management, allowing the application of storage and disposal periods, considering the value of the documents, their potential use in studies and research, and legal and evidentiary issues. The creation and maintenance of these instruments can be the responsibility of a specific committee or body.
- Review of retention periods for imaging test results: Reviewing retention periods for imaging test results is important, as different tests may have different expiration dates, and not all of them need to be kept for 20 years. The suggestion of differentiating the periods based on the information in the medical report, indicating normality, illness, or the need for new tests, is something that should be considered. This would allow for more efficient management of test results, saving space and financial and technological resources.
- Need for periodic evaluation of EHRs: Creating a Document Evaluation and Allocation Committee (CRPAD) to evaluate and allocate EHRs is a recommended practice. At least every twelve months, a regular evaluation would allow the identification of documents that can be eliminated or collected for permanent storage, saving physical and financial resources. This is especially relevant considering the massive amount of images in imaging exams and the growing amount of patient data.
- Strategies to assist in managing EHRs: Effective EHR management involves implementing processes, archival techniques, and technologies that ensure their governance, including organization, curation, security, interoperability, privacy, and a focus on better service provision to patients. In addition, considering financial savings and rationalizing technological resources are relevant aspects, especially in a Big Data environment with an increasing amount of digital health data. Added to this is the growing number of cyberattacks aimed at hijacking and commercializing data on the Dark Web that require using technologies such as private Blockchain, encryption, and data redundancy, among others.

It was also possible to conclude that the importance of updating document management practices should be considered, considering the specific needs of the health area and technological advances. Efficient management of EHRs saves resources and ensures the integrity, security, and accessibility of patients' clinical information, contributing to quality medical care.

Strategies for Archival and Technological Management of EHRs

The research indicated the importance of adopting innovative approaches to meet the needs of Health 4.0, which is characterized by the intensive use of technology and data. Some relevant observations for this are:

- Blockchain and Smart Contracts for interoperability and security: The use of Blockchain technology and Smart Contracts is a promising approach to ensure the security and interoperability of EHRs. Private Blockchain offers a secure environment for controlling and sharing health information, and Smart Contracts can automate processes.
- EHR archival management: Establishing EHR archival management is important for curating health records. Archival professionals are essential in document organization, maintenance, and preservation.
- CDAMS requirements in the certification of electronic health record systems: Including CDAMS requirements in the certification of electronic health record systems is an important measure to ensure compliance and quality in managing health records.
- Monitoring the maturity level in archival and technological management of EHRs: Creating mechanisms to monitor the maturity level in archival and technological management of EHRs is a relevant initiative to assess progress and identify areas that require continuous improvement. Patient Empowerment 4.0: The strategies presented promote patient empowerment 4.0, allowing them greater control over their health data. This can result in more personalized and efficient healthcare.

These considerations indicate a future scenario where EHR management will be more efficient, secure, and patient-centered. The Archivist will play a key role as a curator of these records, while Blockchain technology and Smart Contracts will offer innovative solutions to the challenges of security, artificial intelligence, and connectivity of Health 4.0.

References

Andrew, J., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications, 215*, 103633. https://doi.org/10.1016/j.jnca.2023.103633

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management. *Business & Information Systems Engineering, 1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Berger, M. F., Petritsch, J., Hecker, A., Pustak, S., Michelitsch, B., Banfi, C., Kamolz, L.-P., & Lumenta, D. B. (2024). Paper-and-Pencil vs. Electronic Patient Records: Analyzing Time Efficiency, Personnel Requirements, and Usability Impacts on Healthcare Administration. *Journal of Clinical Medicine*, *13*(20), 6214. https://doi.org/10.3390/jcm13206214

Castells, M. (2012). A sociedade em rede. [The network Society]. In Paz e Terra ebooks. https://ria.ufrn.br/jspui/handle/123456789/1638

Cedro, L. F. dos A. (2020) *Tecnologia blockchain como auxílio para transparência dos resultados de ensaios clínicos* [Blockchain technology as an aid to transparency of clinical trial results.]. Universidade de Brasília, DF, Brasil. http://ppgcinf.fci.unb.br/pt/component/k2/item/4363-tecnologia-blockchain-como-auxilio-para-transparencia-dos-resultados-de-ensaios-clinicos

Conselho Nacional de Arquivos - CONARQ, Câmara Técnica de Documentos Eletrônicos - CTDE, Santos, V. B. D., Rocco, B. C. D. B., Ditadi, C. A. S., Rocha, C. L., Flores, D., Yamaoka, E. J., Lima, J. A. D. O., Sayão, L. F., Braga, M. A. R., Silva, M. D., & Martins, N. D. R. (2020a). Glossário Documentos arquivísticos digitais. https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glosctde_2020_08_07.pdf

Conselho Nacional de Arquivos - CONARQ, Câmara Técnica de Documentos Eletrônicos – CTDE (2020b). Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos – e-arq Brasil. Rio de Janeiro. https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glosctde_2020_08_07.pdf.

DOU (2002) – Diário Oficial da União - Seção 1, número 153, de 09/08/2002 [Official Gazette of the Union - Section 1, number 153, of 08/09/2002] - Imprensa Nacional. (n.d.). https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=184&data=09/08/2002

Duque, C. G., & Lyra, M. R. (2010). O posicionamento da arquitetura da informação na governança de TI [The positioning of information architecture in IT governance]. *Brazilian Journal of Information Science: Research Trends, Marília, 4*(2), 41–46, jun./dez. https://revistas.marilia.unesp.br/index.php/bjis/article/view/504/756

Ferraz, R. N. (2019). As tecnologias envolvendo os contratos inteligentes (smart contracts) e alguns dos impactos nos contratos. [Technologies involving smart contracts and some of the impacts on contracts]. Centro de Ciências Jurídicas, Universidade Federal de Pernambuco, Recife, 2019. https://repositorio.ufpe.br/bitstream/123456789/37502/1/TCC_RobersonNovellinoFerraz_51018543449_31_10_2019.pdf

Goes, A. C., Siqueira, A. L. C., Marcelino, A. S., Balsan, L. A. G., & Moura, G. L. (2013). Os benefícios da implantação de um prontuário eletrônico de paciente [The benefits of implementing an electronic patient record]. *Revista de Administração Hospitalar e Inovação em Saúde, 10*(2), 40–51.

Gomes, D. P. (2018). Contratos ex machina: breves notas sobre a introdução da tecnologia Blockchain e Smart Contracts [Ex Machina Contracts: Brief notes on the introduction of blockchain technology and smart contracts]. *RED – Revista Eletrónica de Direito. Porto*, (3), 40–55. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3352031

Kumar, R., Tripathi, R., Marchang, N., Srivastava, G., Gadekallu, T. R., & Xiong, N. N. (2021). A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. *Journal of Parallel and Distributed Computing*, *152*, 128-143. https://doi.org/10.1016/j.jpdc.2021.02.022

Lopes, L. C. (2013). *A nova arquivística na modernização administrativa* [*The new archival science in administrative modernization*] *(*2nd ed.). Brasília: Annabel Lee/Projecto editorial.

Mayer, A., Costa, C. A., & RIGHI, R. (2020). Electronic health records in a blockchain: a systematic review. *Health Informatics Journal, 26*(2), 1273–1288. https://journals.sagepub.com/doi/pdf/10.1177/1460458219866350

Nabeto, A. M. S. (2020). *A transformação digital no sector da saúde* [*Digital transformation in the healthcare sector*]. Dissertação (Mestrado em Estratégia de Investimento e Internacionalização) – Instituto Superior de Gestão, Lisboa, 2020. https://comum.rcaap.pt/bitstream/10400.26/33074/1/Tese%20Mestrado%20Ana%20Nabeto%2030Junho%202020.pdf

Pang, Z., Yao, Y., Li, Q., Zhang, X., & Zhang, J. (2022). Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm. *IEEE Access*, *10*, 87803–87815. https://doi.org/10.1109/ACCESS.2022.3186682

Poikola, A., Kuikkaniemi, K., & Honko, H. (2021). *Mydata: um modelo nórdico para gestão e processamento de dados pessoais centrado no ser humano* [Mydata: a Nordic model for human-centric management and processing of personal data]. Rio de Janeiro: FGV, 2020. https://internet-governance.fgv.br/sites/internet-governance.fgv.br/files/publicacoes/selection_novo.pdf

Proença, D., Vieira, R., & Borbinha, J. (2018). Avaliação de maturidade da governança da informação em arquivos [Information governance maturity assessment in archives]. *In: congresso nacional de bibliotecários, arquivistas e documentalistas*, 13., 2018, Lisboa. Anais [...]. Lisboa: BAD. 1–9. https://www.bad.pt/publicacoes/index.php/congressosbad/index

Rodrigues, C. (2017). Uma análise simples de eficiência e segurança da tecnologia blockchain [A simple analysis of the efficiency and security of blockchain technology]. *Revista de sistemas e computação, salvador, 7*(2), 147–162, jul./dez..
https://repositorio.uniceub.br/jspui/bitstream/235/11373/1/Uma%20an%C3%A1lise%20simples%20de%20efici%C3%AAncia%20e%20seguran%C3%A7a%20da%20Tecnologia%20Blockchain.pdf

Silva, L. V. G. (2020). Saúde digital: a interoperabilidade e a tecnologia blockchain. Experiência profissionalizante na vertente de farmácia comunitária e investigação [Digital health: interoperability and blockchain technology. Professional experience in community pharmacy and research]. Universidade da Beira Interior, Covilhã. https://ubibliorum.ubi.pt/handle/10400.6/10600

Tracy, D. K., Gadelrab, R., Rahim, A., Pendlebury, G., Reza, H., Bhattacharya, R., … Dave, S. (2024). Digital literacy in contemporary mental healthcare: electronic patient records, outcome measurements and social media. *BJPsych Advances, 30*(1), 36–43. https://doi.org/10.1192/bja.2022.74

Xavier, A. C. & Gottschalg-Duque, C. (2021). Prontuário eletrônico do paciente: qual a contribuição da arquivística e do Smart Contracts para a sua gestão na Era da Saúde 4.0?. AtoZ: novas práticas em informação e conhecimento [Electronic patient records: what is the contribution of archiving and Smart Contracts to their management in the Health 4.0 Era?. AtoZ: new practices in information and knowledge], *10*(3), 1–10. http://dx.doi.org/10.5380/atoz.v10i3.81267

Acknowledgments
Not applicable.

Funding
Not applicable.

Conflict of Interests
No, there are no conflicting interests.