Journal of Public Health (2024) 32:435–454
https://doi.org/10.1007/s10389-022-01795-z

REVIEW ARTICLE

Privacy in electronic health records: a systematic mapping study

Rodrigo Tertulino[1] · Nuno Antunes[2] · Higor Morais[1]

Received: 20 October 2022 / Accepted: 5 December 2022 / Published online: 23 January 2023

Abstract

Main Electronic health record (EHR) applications are digital versions of paper-based patient health information. Traditionally, medical records are made on paper. However, nowadays, advances in information and communication technology have made it possible to change medical records from paper to EHR. Therefore, preserving user data privacy is extremely important in healthcare environments. The main challenges are providing ways to make EHR systems increasingly capable of ensuring data privacy and at the same time not compromising the performance and interoperability of these systems.

Subject and methods This systematic mapping study intends to investigate the current research on security and privacy requirements in EHR systems and identify potential research gaps in the literature. The main challenges are providing ways to make EHR systems increasingly capable of ensuring data privacy, and at the same time, not compromising the performance and interoperability of these systems. Our research was carried out in the Scopus database, the largest database of abstracts and citations in the literature with peer review.

Results We have collected 848 articles related to the area. After disambiguation and filtering, we selected 30 articles for analysis. The result of such an analysis provides a comprehensive view of current research.

Conclusions We can highlight some relevant research possibilities. First, we noticed a growing interest in privacy in EHR research in the last 6 years. Second, blockchain has been used in many EHR systems as a solution to achieve data privacy. However, it is a challenge to maintain traceability by recording metadata that can be mapped to private data of the users applying a particular mapping function that can be hosted outside the blockchain. Finally, the lack of a systematic approach between EHR solutions and existing laws or policies leads to better strategies for developing a certification process for EHR systems.

Keywords Electronic health record (EHR) · Health · Privacy · Security

Introduction

During the last decades, information and communication technology (ICT) has provided healthcare professionals with support in managing research and patient care information. ICTs in the healthcare system have great potential to improve care in developed and developing countries, providing better access to information through the healthcare system (Pai et al. 2021).

Healthcare institutions have been invested in healthcare information technology to improve care, quality, and reduce operating costs (Berner et al. 2005). Thus, some studies indicate that the implementation of the Health Information System (HIS) increases the quality of patient care and safety by reducing medical errors, hence improving the institution’s performance, reducing treatment costs, and, at the same time, saving resources of medical institutions and health (Ahmadian and Khajouei 2012; Tan 2008). In addition, these systems can raise the readability of recorded data, decrease medical errors, and ultimately lead to user satisfaction (Ahmadian et al. 2015).

However, excellence in patient care depends directly on the ability of healthcare systems to collect, store,

✉ Rodrigo Tertulino
rodrigo.tertulino@ifrn.edu.br

[1] Federal Institute of Education, Science, and Technology of Rio Grande do Norte (IFRN), Natal, Brazil

[2] Department of Informatics and Engineering of the University of Coimbra (UC), Coimbra, Portugal

access, analyze, and transmit information about patient health data electronically. ICTs have the potential to significantly contribute to preventive care, improving healthcare service delivery, disease control, health management, and research (Balsari et al. 2018).

Thus, healthcare systems comprise various people who make up this system, such as pharmacists, laboratory technicians, physicians, nurses, radiologists, and patients. Information collected in hospitals and physicians' offices during clinical meetings is typically managed, stored, and maintained by hospitals for a more extended period to provide care and follow-up to the patient. Due to the large amount of data, hospitals sometimes find it challenging to store and manage patient health data.

The healthcare system is a term used to refer to all systems that are part of the healthcare domain. Hence, a large variety of devices are now available, including health trackers, IoT devices, and smart watches (Wazid et al. 2018), which are being used by patients to monitor daily activities and measure personal data, such as blood pressure, heart rate, electrocardiogram (ECG) and breath analysis. Currently available wearable devices (WDs) are delivered as wireless devices that are placed directly on the patient's body (Hathaliya et al. 2020). Thus, contemplating the systems that are part of this environment, we can thus highlight the electronic health record (EHR) responsible for handling and storing the most sensitive information patient such, medications, progress reports, vital signs, medical history, immunization reports, laboratory data, and radiology reports (Keshta and Odeh 2020).

Electronic health records (EHR) are commonly used to store patient data within healthcare providers. EHR systems provide storage and management of patient data inside and between institutions (Hussienet al. 2019).

It is estimated that clinical data will increase to 2314 exabytes by 2020, from 153 exabytes in 2013 each year, and the growth rate is 48%. Hence, this number is increasing exponentially. (Pramanik et al. 2019). However, there are privacy concerns about the EHR systems (Yksel et al. 2017).

Traditionally, medical records have been recorded on paper. However, nowadays, advances in information and communication technology have made it possible to change medical records on paper to an electronic version of the medical record (Nweke et al. 2020). Thus, like the traditional paper medical record, an electronic version of the record is a set of information such as recording an individual's medical history. Unlike conventional paper medical records, the electronic version is stored in electronic format. The electronic version of medical records is called electronic health records (EHR) (Nweke et al. 2020).

Electronic health records (EHR) are increasingly being used by patients, hospitals, doctors, and other health professionals. EHR have several advantages, such as reduced health costs and more efficient availability in relation to the processing of stored records. On the other hand, the use of EHRs raises concerns about the safety, privacy, and integrity of patient records. These concerns affect patients' interest in disclosing their health data and can have fatal consequences. For example, the United States Department of Health and Human Services (HHS) estimated that approximately 2 million Americans with mental illness did not seek treatment precisely because of privacy concerns (Yüksel et al. 2017).

In this context, the EHR system has grown as a solution for storing and managing users' private health data (Keshta and Odeh 2020). Hence, much research has been done to ensure the privacy of this information within the EHR system (Smaradottir 2018).

This article aims to examine the current research state of the art about privacy in electronic health records. Furthermore, we will research the EHR system's main requirements proportionate to the users, based on existing legislation and policy. Thus, these requirements must be followed to provide privacy to users who use these systems. To achieve this goal, we adopted a systematic mapping process based on the work of Petersen (Petersen et al. 2015; Petersen et al. 2008). From systematic mapping, we can better understand what the main challenges of the academic community are and what the main solutions being proposed are. Mapping studies provide a good overview of a research subject and are helpful before starting deeper research works (Hakim and Sensuse 2018).

Our analysis will show the growth of solutions to provide privacy in the EHR system. We will also present the main challenges and what methods are being used to provide privacy in the EHR system. At the same time, we research based on legal and ethical questions (legislation and policy) in the EHR system. Thus, the study aims to understand the current state and future trends in the privacy of EHR systems. In addition, to achieve this goal, we carried out a systematic mapping. In Section "Methodology" we will see more details about our research methods.

The rest of this paper is organized as follows. Section "Privacy in electronic health records" presents some background about privacy in electronic health records. Section "Methodology" introduces the methodology adopted for map construction. Section "Results" presents the results in terms of the papers gathered from the scientific databases. Section "Mapping" presents the maps collected. Section "Discussion" discusses the maps and the main considerations. Finally, Section "Conclusions" concludes the study paper.

Privacy in electronic health records

The Organization for Economic Co-operation and Development (OECD) has long recognized the vital role of privacy as a fundamental value and condition for the free flow of personal data across borders. The main objective was to provide a set of guidelines in order to protect the privacy and, at the same time, promote a free flow of information. Thus, to achieve these goals, the guidelines establish set principles for member countries to use as a basis for national laws worldwide. Thus, OECD Guidelines contribute significantly to the construction of laws such as GDPR (Horodyski 2015).

The United Nations General Assembly (UNGA) declared that privacy is essential to the Declaration of Human Rights. Nevertheless, in this digital age, the term privacy has become subjective and defined by each state or country (Kayaalp 2018). Hence, the privacy of clinical data has been subject to many studies (Kho et al. 2015).

It has not been easy to settle how much the data belongs to the patient and how much it can belong to health institutions, and whether the data owner's consent is required if the data is used for study (Richter et al. 2019).

The data collected must be protected against unauthorized access to ensure the privacy of the information and, at the same time, ensure the preservation of the information (Aslam et al. 2019). The use of this medical data should be available only for the purposes for which the patient has given consent (Jayabalan and O'Daniel 2017). In addition, data access must follow the rules and procedures to ensure access to the patient's medical data, either by authorized persons or only by applications (Kadhim et al. 2020).

Health information technology refers to all information technology systems used to store, access, process, share, and transmit information or enable support for health care provision and the health system's management. Thus, the information that health information technology contains is highly sensitive (Kadhim et al. 2020). The information includes data related to diseases, diagnoses, exams, and treatments carried out, all together with information about the patient's medical history (Häyrinen et al. 2008). Therefore, this information must be protected not to be manipulated, allowing patients to continue sharing information about their health and work, considering the moral and legal responsibilities. Hence, ensuring that health records are private is negatively impacted by the health information's dynamic nature (Sittig and Singh 2010).

The common issues that need to be approached in the electronic health record EHR system are privacy, security, and confidentiality (Alanazi et al. 2015). Even though privacy and security are deeply related, they are in a real sense, different. Security is defined as how accessing someone's personal information is restricted and allowed for only those authorized. On the other hand, privacy refers to the right that somebody has to determine for themselves when, how, and the level at which accessing private information is transferred or shared by others (Sittig and Singh 2010).

Privacy laws and regulations for health

Privacy policies have been duly legalized in several countries to grant controller and protect patient records' privacy. The Health Insurance Portability and Accountability Act (HIPAA) protects information related to users' health data stored or transmitted by the institution, by any means, whether electronic, paper, or oral. The privacy rule is also known as protected health information (PHI) (HIPAA 2013b). In recent years, the EU data protection directive 95/46/EC, applied to EHRs data privacy, is replaced by General Data Protection Regulation (GDRP) (Shah and Khan 2020). The goals of the GDPR are to secure consistent data protection rules in Europe, propose reinforcement and redesign individuals according to their private data, and improve the process of data flows (Kanwal et al. 2020). GDPR's jurisdiction spreads to all companies that own or process citizens' personal data in EU countries, regardless of the company's location. Hence, it expands the scope of the law for organizations outside the EU that offer goods or services, or monitor EU citizens' behavior. Staggered penalties are assessed based on the nature of the infringement and the organization's revenue (Kloss et al. 2018). Based on the European regulation (GDPR), in Brazil the (General Personal Data Protection Law - LGPD) determines rules for collecting, handling, storing, and sharing personal data managed by organizations. In August 2018, the corporation will have 18 months to adjust to the new rules with presidential approval. Hence, this law came into force in August 2020. Among the actions toward the LGPD are collecting and using personal data without the consent of both the private sector and public authorities and the use of personal information for practicing unlawful or unfair discrimination.

The laws mentioned above were created to offer security and privacy requirements for any system. HIPAA is more focused on personal health information (PHI) on systems in the healthcare domain. Meanwhile, GDPR and LGPD are aimed at systems in general, without being specific to any system.

We can notice that there is a mix-up among requirements, standards, laws, rules, policy, and guides. Hence, it is not straightforward to even distinguish them. In order to try to establish a pattern, first we need to define the meaning of each. Thus, the requirement indicates a condition or characteristic the system must conform to. In contrast, a standard can be defined as a set of specifications that determine the compatibility of different products. The laws correspond to what was regulated and established by legislators and are part of the set of rules of law. On the other hand, a rule is a norm or order of behavior dictated by a competent authority whose non-compliance or ignorance results in applying a specific sanction. As long as the guidelines are general suggestions, they are not mandatory or required. Unlike policies that are standardized requirements that apply to a specific area or task, they are mandatory and required. In comparison, the policy is a set of ideas or a plan of what to do in certain situations that have been approved to officially by a group of people, a company institution, a government, or a political institution.

LGPD, GDPR, and HIPAA are conceptually laws, while NIST and ONC can be classified as rules because they are not mandatory as a law. However, we treat them all as requirements for analysis and study purposes because they are characteristics that systems must have, such as the right to be forgotten, access control, integrity, de-identification, encryption, and so on.

Thus, as a way to improve understanding, adoption of privacy and security requirements were created with this purpose, such as the Health Information Technology for Economic and Clinical Health Act (HITECH), Office of the National Coordinator (ONC), and National Institute of Standards and Technology (NIST). HITECH's main objective is to provide an improvement in quality and security for systems that process health data (Al-Issa et al. 2019). It acts as law and was created by the U.S. Department of Health and Human Services (HHS) with the intent of expanding the adoption of EHR use by healthcare providers, also offering financial incentives for providers to adopt these systems as soon as possible (Shah and Khan 2020). However, HITECH serves as a kind of addendum to HIPAA.

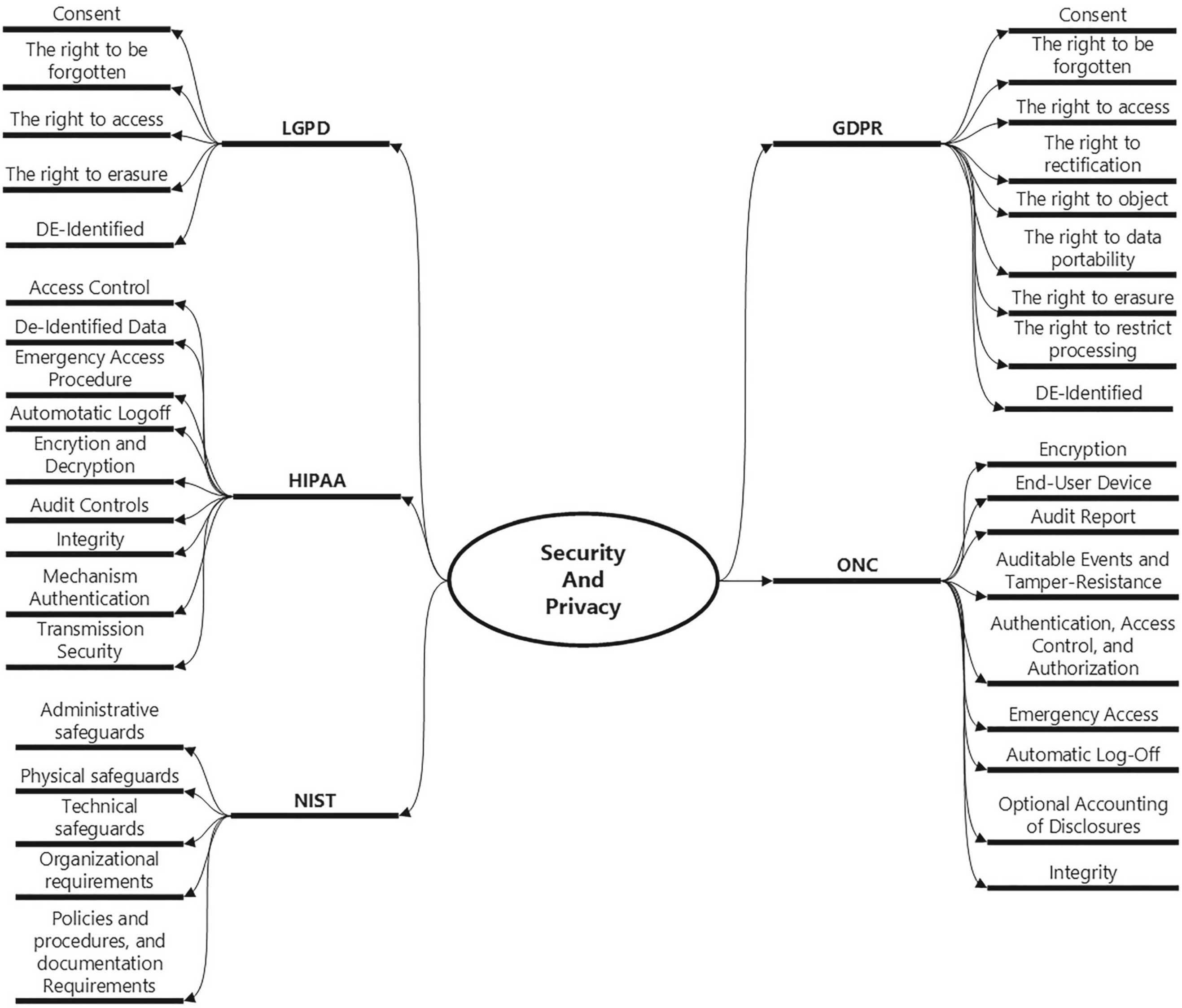


Fig. 1 Overview of the main security and privacy concepts mentioned in the standards

It states that all technology standards from HITECH must comply with HIPAA's Privacy and Security Rules. At the same time, the (ONC) for Health Information Technology (HIT) provides a certification program that sets criteria toward the usability aspects of EHRs (Farhadi et al. 2019). Besides that, the (NIST) has also developed a guide for the implementation of guidelines based on HIPAA, in which the guidelines are demonstrated, categorizing them into administrative safeguards, physical safeguards, technical safeguards, organizational requirements and policies and procedures, and documentation requirements (Scholl et al. 2008).

However, HIPAA, NIST, and ONC bring more specific security and privacy requirements that systems like EHRs must have. Hence, laws like GDPR and LGDP have more comprehensive requirements that do not just include systems that are part of healthcare.

Thus, we can see in Fig. 1 the main concepts that are mentioned and required of existing legislation and policy regarding the security and preservation of users' privacy.

Privacy concerns in EHRs

Hence, it is not easy to balance privacy and usefulness; protecting EHR data is not a simple task. When patient data are publicly available, they need to be protected against many privacy threats, such as identifying the disclosure of confidential patient information. At the same time, patient-specific information would be useful for subsequent analyzes (Gkoulalas-Divanis et al. 2014).

Clinical data based on EHR offer several advantages when compared to manual medical records. Hence, it substantially improves the overall quality of health. In addition, it becomes easily accessible through various means of communication (Amato et al. 2015). All of these advantages encourage healthcare providers and doctors to adopt an EHR system (Guo et al. 2018). However, the adoption of EHR and its data processing presents several privacy problems, especially when these data are used, shared, or even accessed by those who should not have access (Shah and Khan 2020).

Transferring or sharing confidential health information when not authorized, may lead to a data breach. Privacy can also be violated in many other situations, for example, by identifying and registering patients' access when using the system. However, in some cases, the government, researchers, pharmaceutical companies, and laboratories may have valid reasons for accessing patients' health records to obtain some data. In the process, the health provider may abuse the accidental or intentional access to health records (Cifuentes et al. 2015).

EHR data are the data most vulnerable to cyber threats. The main reason why criminals target medical data is to obtain financial benefits. Hence, criminals sell the valuable data obtained from the EHR to the "dark web" and have obtained considerable economic benefits. Thus, for criminals, EHR data are more valuable than credit cards because it contains various fixed identifiers and essential financial information, further precious in the black market (Shah and Khan 2020). We can also point out that one of the biggest problems is the lack of trust and privacy requirements (Odeh et al. 2022).

Identification of relevant studies

Recent papers tackled such challenges. For example, in the papers (Fernández-Alemán et al. 2013) and (Mehndiratta et al. 2014), the authors present the difficulties of providing security and privacy in EHR systems.

Whereas (Edemacu et al. 2019) propose an overview of ways to provide privacy in EHR based on access control methods (encryption-based methods and independent encryption methods). Meanwhile, the authors (Shrestha et al. 2016) propose a safe health system against attacks by unauthorized users. Other articles have systematically analyzed regulation and enlisted their challenges for ensuring data privacy in this era where EHR usage (Shah and Khan 2020). The article cites the matter of EHR systems within the healthcare environment. In addition, studies have been done on technological procedures to achieve privacy when sharing EHR, ranging from traditional to advanced cryptographic techniques encryption standard (AES) (Aldossary and Allen 2016). In this article, the authors discuss the standards that can be used to protect the anonymity and privacy of medical data (Aslam et al. 2019). Hence, techniques have been proposed to preserve the privacy of a patient's data, such as authentication, encrypting the data, data masking (K Anonymity, L Diversity, T Closeness), and access control (Rana and Jayabalan 2016). These methods provide sharing, storage, data collection, and privacy to EHRs through encryption. Meanwhile, research that uses blockchain has been extensively explored, as we can see in the articles (Sharma and Balamurugan 2020; Sun et al. 2018; Ismail and Materwala 2020).

A systematic mapping looks at state of the art, emphasizing what the researcher needs to obtain from the information. Consequently, checking who the authors are, who are the authors who most publish on the researched topic, which are the institutions, the years of publication, the research methods, which conferences and journals other researchers publish, which questionnaires are used, and investigated variables (Hakim and Sensuse 2018). A systematic review is a way to evaluate and understand all the research essential to a research question, subject, or phenomenon of particular interest (Kitchenham 2004). The systematic mapping has a focus on specific aspects

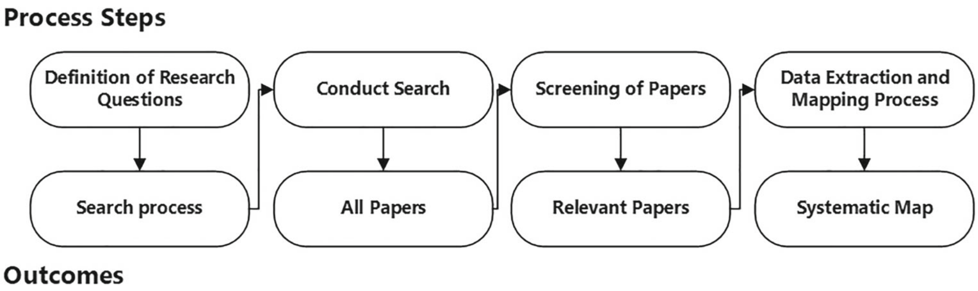


Fig. 2 Systematic mapping process

of the researched subject, as well as a detailed analysis of the articles. Thus, we can say that a systematic mapping provides a quicker result compared to a systematic review.

Methodology

The systematic mapping process is based on the work of Petersen et al. (2008, 2015). Figure 2 shows the steps and results of the process described in the following sections.

Research questions

This systematic mapping study's main objective is to provide an overview of recent research on privacy mechanisms in electronic health records (EHR). Hence, the study aims to understand the current state and future trends on EHR systems privacy. The steps of the systematic mapping study method are documented in the following research questions:

- **RQ1**: What are the main privacy challenges related to EHR?
- **RQ2**: What are the main requirements identified by the laws that EHR systems should respect?
- **RQ3**: What are the main published techniques to provide privacy in the EHR system?
- **RQ4**: How well are the published techniques addressing the requirements?

Search process

Our research was carried out in the base Scopus (Elsevier), the largest database of abstracts and citations in the literature with peer review: scientific journals, books, conference proceedings, and industry publications which index the main sources. We decided not to search in other databases like Google Scholar because we only wanted publications with peer review. Examples of sources indexed by Scopus (Elsevier) are shown in Table 1.

To define the search string, we used terms related to the healthcare domain, privacy, and electronic health records. The main goal was to obtain significant research on these terms. Thus, the defined search string was:

- (“Privacy” AND “Healthcare” AND “Electronic Health Records”)

We did not include laws or policies as a search criterion because we wanted to research whether the proposals to provide privacy and security in these articles followed the regulations set out in the laws and policies mentioned earlier.

The first part of the research sequence is related to the privacy aspects, specifically because our main intention is to find out the main challenges toward privacy regarding electronic records. In order to establish and limit the number of articles retrieved from using the search string, we used a search option with a refined or filtered search option into database sources.

The second part of our research was related to the health domain because we want to focus our research in a way that can bring results closer to our purpose.

In the third part of the search string, our target is electronic health record systems. Other terms have been omitted, such as medical record systems or health records and personal health record systems because they have different purposes from EHR systems inside the healthcare domain.

Quality assessment

Each selected study was evaluated according to the following quality assessment (QA), Questions:

- **QA1.** Is the paper based on research (or is it merely a “lessons learned” report based on expert opinion)?

Table 1 Examples of sources indexed by Scopus (Elsevier)

Source	Link
ACM Digital Library	http://dl.acm.org
IEEExplorer	http://ieeexplore.ieee.org
Science Direct	http://www.sciencedirect.com
Springer Link	http://link.springer.com

- **QA2.** Is there a clear statement of the aims of the research?
- **QA3.** Is there an adequate description of the context in which the research was carried out?
- **QA4.** Is the study of value for research or practice?
- **QA5.** Is there a clear statement of findings?

These criteria were based on (Dybå T and Dingsøyr T 2008), and on three circumstances that need to be addressed regarding literature review studies:

- **Rigor:** A complete and appropriate approach was applied to the research methods essential in the study?
- **Credibility:** Are the findings well presented and significant?
- **Relevance:** How useful are the findings to the software and the investigation community?

Screening of papers

We establish the inclusion and exclusion criteria to filter the search results. Our goal is to select relevant EHR privacy articles over the past 6 years. Thus, our article selection process intends to cover peer-reviewed articles on the subject. The research on privacy in EHR brought us many sources; for this reason, we decided to limit our research only to articles published in journals and conferences indexed based on Scopus (ELSEVIER). Finally, we also removed the review articles, as we intend to analyze the articles' individual contributions instead of a compilation of articles. In order to get the appropriate papers in this systematic literature review, we decide the criteria for inclusion and exclusion. The filtering strategy adopted is summarized below.

- **Inclusion criteria** This review included published works limited to results from fonts written between 2015 and 2021. Written in English. We have limited only articles published in journals or conference papers. Articles focused on privacy, healthcare, and electronic health records in their titles, abstracts, keywords, or introductions were taken into account
- **Exclusion criteria** Articles that did not have an electronic health record and where the researchers did not have access, were excluded from the review, as well as papers not written in the English language, review, and surveys, books and gray literature, Informal literature surveys.

The data extracted from each study were: authors country, publication year, venue (journal of conference), goal, privacy, electronic health records, healthcare, legal ethical questions (laws), challenges, future work and additional comments.

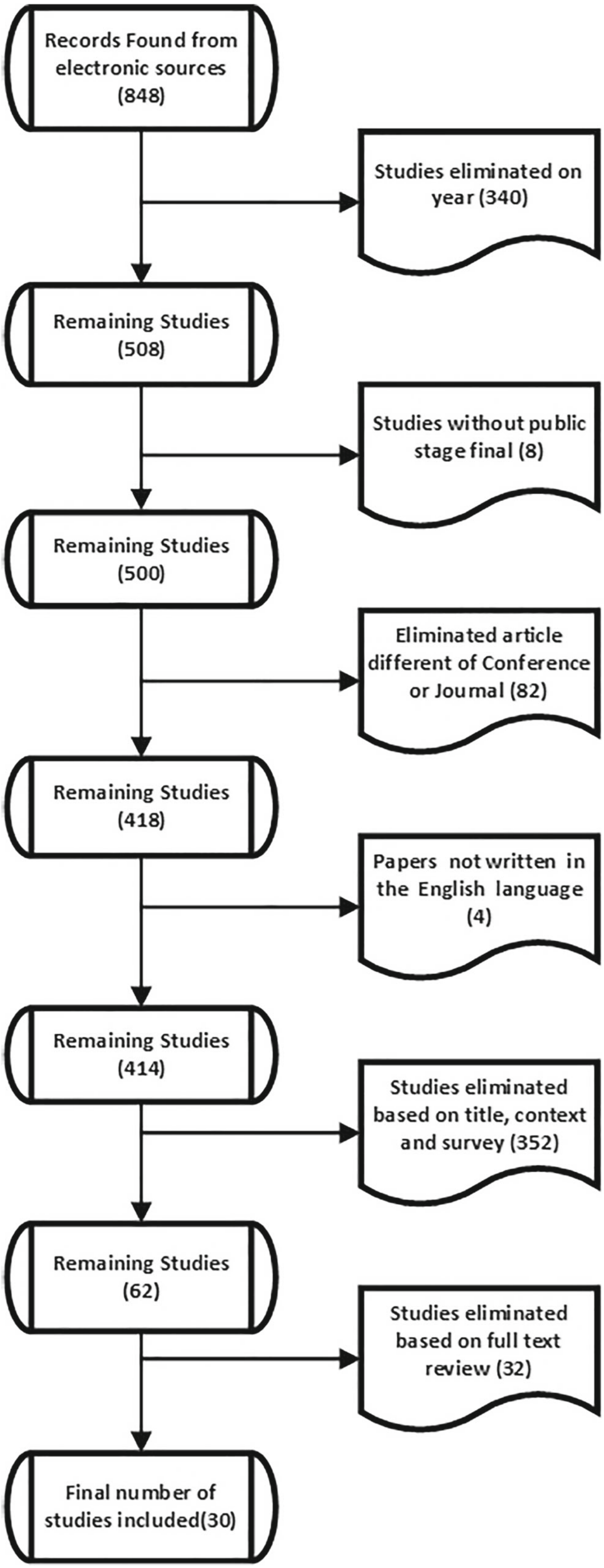

Records Found from electronic sources (848)
Studies eliminated on year (340)
Remaining Studies (508)
Studies without public stage final (8)
Remaining Studies (500)
Eliminated article different of Conference or Journal (82)
Remaining Studies (418)
Papers not written in the English language (4)
Remaining Studies (414)
Studies eliminated based on title, context and survey (352)
Remaining Studies (62)
Studies eliminated based on full text review (32)
Final number of studies included(30)

Fig. 3 Paper selection process

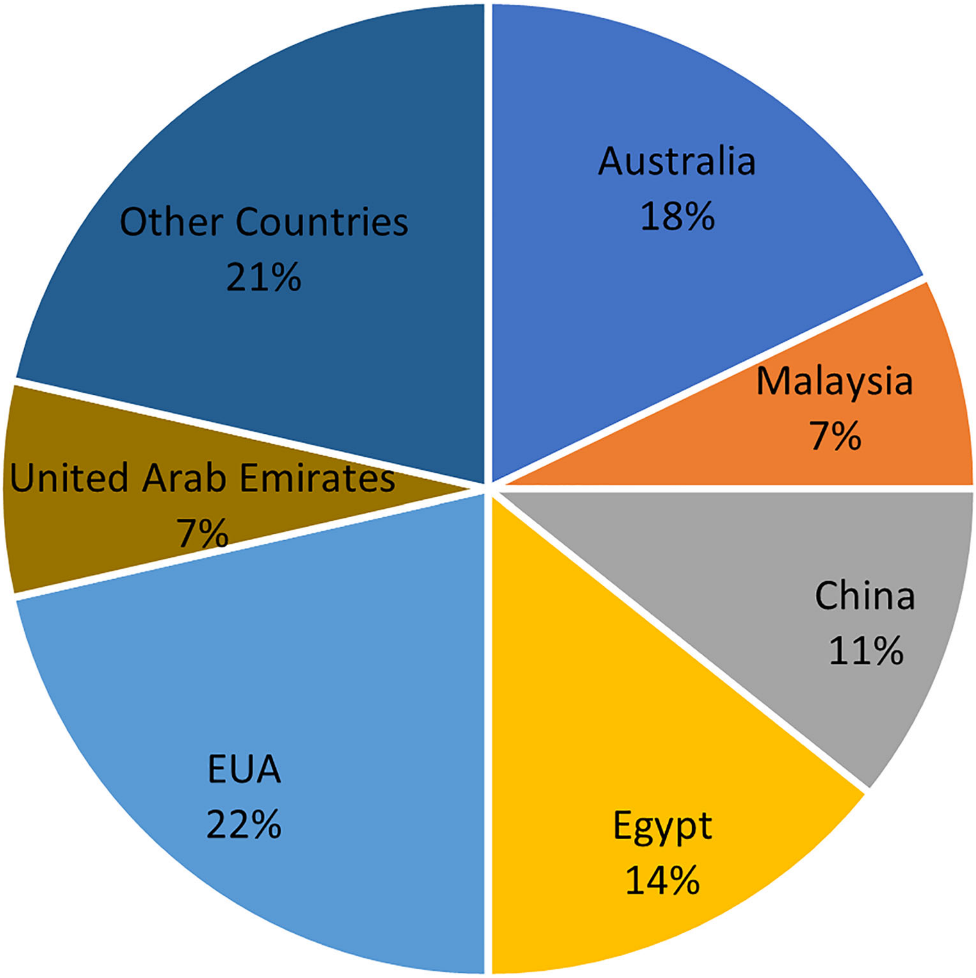
Results

The search was made between October 16 and 14 of November 2021 and resulted in 848 papers. The first step was to eliminate articles published before 2015 in an automated way through Scopus' own search engine filters. Similarly, through filters, we eliminated articles that were not in the final stages. We also eliminated articles from different journals and conferences. Then, articles that had no English language were eliminated. After further detailed reading of the article's abstract, we deleted articles that did not meet our research objective according to the quality assessment. This final step involved obtaining, reading, classifying, and analyzing, as illustrated in Fig. 3, and 62 remaining articles were obtained in the full-text version. As such, a full-text reading was performed in each study to verify that the article met all the study requirements. Once the articles were read thoroughly and carefully, the final list was reduced to 30 references. This reduction was due to the following aspects:

- **5** articles were excluded because the studies are surveys;
- **7** articles were excluded because the studies are systematic reviews;
- **8** articles were excluded because the studies were not conducted in privacy;
- **12** articles were excluded because they did not present a proposal to deal with privacy in EHR systems.

In Fig. 4, we can highlight the countries of origin of the authors with more publications, thus as we can see EUA with 22%, followed Australia with 18% on the leader, after Egypt with 14%, China with 11%, and followed by the United Arab Emirates with 7%. Meanwhile, only one author was classified with others and this adds up to a total of 21%.

Fig. 4 Countries by authors



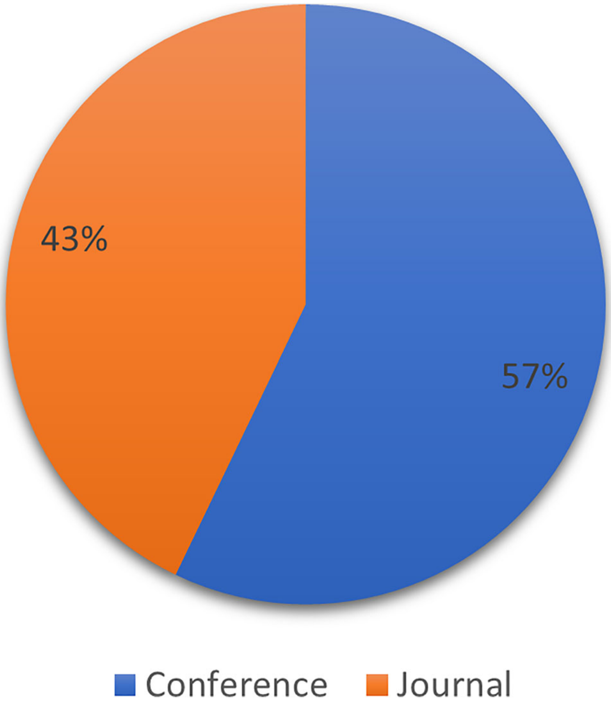


Fig. 5 Venue types

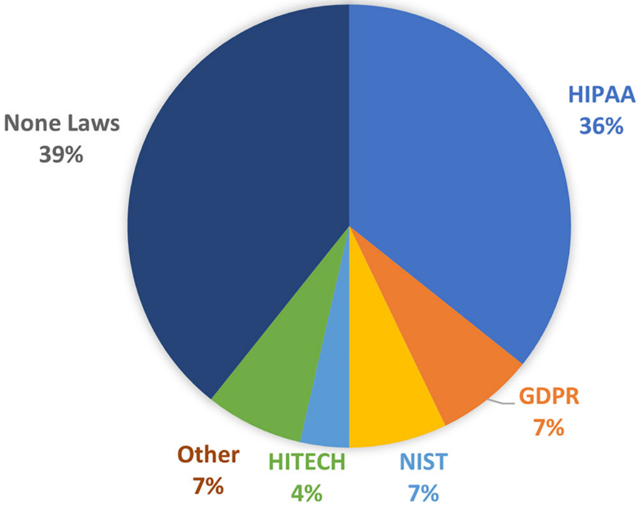


Fig. 6 Classification of papers

We also investigated the frequency of articles according to the type of publication forum. Figure 5 presents the proportion of articles distributed in the two types of forums: journals and conference articles. Thus, 17 represent 57% of papers found at conferences, and 13 represent 43% of papers found in journals. Hence, this shows a balance between these two types of forums. Each article was classified as shown in Section "Methodology".

Rank venues of publication

In our study, our search focused on the Scopus database, which indexes several other databases. Thus, we can see that IEEE is the journal with the largest number of sources. The other sources have only referred to an article, so we declare it as other forums. This shows that our research has returned many journals and several conferences; this helps to guarantee and highlight the degree of reliability of the research method.

Our classification was made based on the laws and policy highlighted previously. Hence, we can select the articles and review the privacy requirements if they were met in the articles. Figure 6 shows that HIPAA 36% holds the main law mentioned in the articles, followed by GPDR with 7%, NIST 7%, and other with HITECH 4%. We can highlight that the largest number of articles with 39% did not mention any law or policy as a basis for building their solutions. We can also see that other laws were cited, representing 7% of the articles. Also, LGPD and ONC were not mentioned in any of the selected articles.

Classification

We summarize the requirements (Gardiyawasam Pussewalage and Oleshchuk 2016; Shah and Khan 2020; HIPAA 2013b); and (HITECH 2009) that must be met based on the legislation and policy Fig. 1 that are important when performing the next-generation EHR systems to guarantee data privacy. Our purpose is to analyze the main security requirements as a way of guaranteeing to preserve privacy. These requirements provide a way to cover the most significant aspects of each article regarding our research questions. Our classification approach is transversal in all selected proposals, which means that an article can comprise more than one requirement. Aspects of each requirement are discussed in the following paragraphs.

Access control

EHR systems must have means that allow access control of data access to preserve patient privacy by employing rules and restrictions for private data access, hence being considered compatible with the requirements demanded by HIPAA to access users' health data (Gardiyawasam Pussewalage and Oleshchuk 2016).

Emergency access

Systems should provide access to patients' PHI information during an emergency. Access controls are necessary to make it possible in cases of emergency conditions, although they may be very different from those used in normal operating circumstances (Farhadi et al. 2019).

De-identification

De-identification allows PHI to be shared without breaking patients ‘privacy or requiring users’ consent or prior authorization from the patient. The information can be useful after being de-identified for studies, medical research, or health policy assessments (Grana and Jackwoski 2015).

Audit control

Auditing is a security measure that enables a healthcare system to provide security for data. Auditing means keeping a record of all users’ activities in a way that makes it possible to track any information accessed, modified, or deleted (Hussien et al. 2019). At the same time, systems like EHR should offer the option of traceability as a way of providing privacy.

Integrity

PHI information that is improperly altered or destroyed can result in clinical quality problems for a provider, including patient safety issues. Thus, any tampering or modification of data is prohibited by laws. In addition, data shared between entities must originally represent information, that is, without modifications (Gardiyawasam Pussewalage and Oleshchuk 2016). Hence, other entities cannot access the data without the user’s consent. Besides, the data must be protected against modifications (Shah and Khan 2020).

Secure transmission

A secure data transmission technique is intended to implement technical measures to protect against unauthorized access to PHI transmitted over communication networks.

Authentication

Authentication aims to implement electronic mechanisms to ensure that the patient’s PHI is protected and has not been altered or destroyed without authorization. Once covered entities identify risks to the integrity of their data, they must identify security measures that will mitigate the risks (Farhadi et al. 2019).

Consent

The Health Insurance Portability Accountability Act (HIPAA) and the European Data Protection Act require patient consent for your data to be shared with insurance agencies and research organizations (Jayabalan and Rana 2018). Healthcare users can terminate their consent at any time, even before the consent has expired (Zhang et al. 2016). Laws such as GDPR and LGPD pertain to the patient being given the right to delete his data whenever he wishes.

Encryption and decryption

Encryption mechanisms should be implemented as a way to protect and safeguard information stored or transmitted whenever possible (Gardiyawasam Pussewalage and Oleshchuk 2016).

Automatic Logoff

EHR should provide a means to log users off automatically after a specified period of inactivity as a way to avoid improper access to user data, thus preserving the privacy of information (Farhadi et al. 2019).

Mapping

This section compares the privacy preservation mechanisms discussed earlier according to our classification in Section “Methodology”. For comparison, we use security and privacy requirements, which are: Access Control (AC), Emergency Access (EA), De-identification (DE), Audit Control (AD), Integrity (IN), Secure Transmission (ST), Authentication (AU), Consent (CO), Cryptography and Decryption (ED), and Automatic Logoff (AL). In addition, the results of the comparison are tabulated in Table 2, and we use ‘$\surd$’ to denote satisfaction of a security and privacy requirement, while ‘$\circ$’ is used to denote a lack this requirement in the article. According to the comparison, it is clearly evident that most schemes adhere to the security and privacy requirements considered to a greater extent, but not completely.

Table 2 presents a comparison of the main way for the preservation of privacy and the main requirements. Next, we show the individual researchers who have either defined or researched each of the defined privacy requirements.

Access control

Access control is quite common not just in EHR systems. It is a common method of providing authorized access only to those who must have the right access. Access control is considered a minimum requirement that any EHR must have, so we can see that the vast majority of articles meet the requirement to have access control. Attribute-based access control (ABAC) is a method capable of managing user access, which depends on users, object attributes, and

Table 2 Comparison of privacy preservation requirements

Solution	Mechanisms	AC	EA	DE	AD	IN	ST	AU	CO	ED	AL
Kho et al. (2015)	DCIFIRHD	∘	∘	√	∘	√	√	∘	∘	√	∘
Yang et al. (2015)	Privacy policies	√	∘	∘	∘	∘	√	∘	∘	∘	∘
Amato et al. (2015)	RBAC	√	∘	∘	∘	∘	∘	∘	∘	∘	∘
Rezaeibagha and Mu (2016)	RBAC	√	∘	∘	∘	∘	√	∘	∘	∘	∘
Ibrahim and Singhal (2016a)	Cryptographic	√	∘	∘	√	√	√	√	∘	√	∘
Ibrahim and Singhal (2016b)	Cryptographic	√	∘	∘	∘	√	∘	∘	∘	√	∘
Lu and Sinnott (2016)	XACML	√	∘	∘	∘	∘	∘	√	∘	∘	∘
Zhang et al. (2016)	CBAC	√	∘	∘	∘	√	∘	√	√	∘	∘
Eom and Lee (2016)	PC-ABE	√	√	∘	∘	√	∘	∘	∘	√	∘
Mamun and Rana (2017)	PCEHR	√	∘	∘	∘	√	√	√	∘	√	∘
Poulis et al. (2017)	RT-datasets	∘	∘	√	∘	∘	∘	∘	∘	∘	∘
Tasatanattakool and Chian (2017)	RBAC	√	∘	√	∘	√	∘	∘	∘	∘	∘
Jayabalan and O’Daniel (2017)	RBAC	√	∘	∘	∘	√	∘	√	∘	∘	∘
Sun et al. (2018)	Blockchain	√	∘	√	∘	√	√	∘	∘	√	∘
Vora et al. (2018)	Blockchain	√	∘	∘	∘	√	∘	∘	∘	√	∘
Jayabalan and Rana (2018)	PPDP	∘	∘	√	∘	∘	∘	∘	∘	∘	∘
Abomhara et al. (2018)	WBAC	√	∘	∘	∘	∘	∘	∘	∘	∘	∘
Guo et al. (2018)	Blockchain	√	∘	√	∘	√	√	∘	∘	√	∘
Huang et al. (2019)	Blockchain	√	∘	∘	∘	√	√	√	∘	√	∘
Nortey et al. (2019)	Blockchain	√	∘	∘	∘	√	∘	∘	∘	√	∘
Shahnaz et al. (2019)	Blockchain	√	∘	∘	∘	√	√	∘	∘	√	∘
Xu et al. (2019)	PR-CP-ABE	√	∘	∘	∘	√	∘	∘	∘	√	∘
Essa et al. (2019)	Apache hadoop, IFHDS	√	∘	∘	∘	√	∘	∘	∘	√	∘
Nguyen et al. (2019)	Blockchain	√	∘	∘	∘	√	√	√	∘	√	∘
Verdonck and Poels (2020)	Blockchain	√	∘	∘	∘	√	√	∘	√	√	∘
Ismail and Materwala (2020)	Blockchain	√	∘	∘	∘	√	√	∘	∘	√	∘
Al Baqari and Barka (2020)	Blockchain	√	∘	∘	∘	√	√	√	∘	√	∘
Sharma and Balamurugan (2020)	Blockchain	√	∘	∘	∘	√	∘	∘	∘	√	∘
Zaabar et al. (2021)	Blockchain	√	∘	∘	∘	√	∘	√	∘	√	∘
Jagtap et al. (2021)	Blockchain	√	∘	∘	∘	√	∘	∘	∘	√	∘

Legend: AC - Access Control, EA - Emergency Access, De-identification (DE), Audit Control (AD), Integrity (IN), Secure Transmission (ST), Authentication (AU), Consent (CO), Encryption and Decryption (ED), and Automatic Logoff (AL)

a set of rules and policies that can define how access will be performed. However, ABAC is not yet formally standardized (Gardiyawasam Pussewalage and Oleshchuk 2016). NIST has standardization and a set of guidelines to formalize and guide on how to implement ABAC (Hu et al. 2014). Meanwhile, some methods present an approach making use of access controls through Role-Based Access Control (RBAC), such as (Amato et al. 2015) proposes a hybrid framework toward permitted and supporting the definition of detailed access control policies running on semi-structured EHRs through a customized RBAC model to improve access to parts of semi-structured EHRs. In this paper, (Tasatanattakool and Chian 2017) propose using algorithms and RBAC to protect patients’ privacy in e-health systems. The proposed algorithms are to protect a patient’s health records. On the one hand, role-based access control is used to classify the authorized users when it comes to using a patient’s health records. We also studied the evolution of this model that started to use other techniques to control access, such as (Jayabalan and O’Daniel 2017). This work presents a study on the access control framework for EHR. Information access control is essential for protecting patient privacy and security. Usually, access control is a blend of many elements, such as authentication, authorization, and compliance detection (audit trails), which form the information security ecosystem. The authors (Nguyen et al. 2019) propose a new architecture for sharing EHR based on a blockchain network. In this paper, the authors develop a reliable access control mechanism based on a single, smart contract to control user access to ensure efficient and secure EHR sharing. For this, they developed a reliable mechanism using smart contracts. Smart contracts define all operations that are allowed in access control. At the same time, users can interact with smart contracts at the contract address. Thus, the prevention of data privacy was possible through the use of blockchain and smart contracts. Furthermore, it was possible to offer an access control scheme guaranteeing data privacy and data ownership of individuals.

In this article (Nortey et al. 2019), a blockchain framework is proposed for controlling EHR data over a distributed network to ensure users' sensitive health data privacy, hence allowing the patients to control access to their data stored in the EHS system. This article (Verdonck and Poels 2020) aims to offer an alternative to manage EHRs with blockchain technology through smart contracts, thereby facilitating patient permissions on patients' healthcare records. Requests are sent to patients who can decide to grant or deny the patient's medical record request. When a request is accepted, the data controller who stores the respective record is notified by a smart contract to add read/write rights to the respective healthcare provider for granted patient record. This article (Jagtap et al. 2021) describes a strategy to protect health data. The proposed model's key features are interoperability, secure storage, and access to patient data. The authors presented an approach to medical records management using smart contracts to provide audibility, interoperability, and usability. This system, intended to document flexibility and granularity, allows for data exchange and encourages the medical examination system. The authors (Rezaeibagha and Mu 2016) present an access control mechanism for an EHR system with a hybrid cloud structure, which allows dealing with many users with different access privileges. The policy transformation approach allows EHR data to be transferred from a private cloud to a public cloud with the corresponding transformation in access control policy. Thus, for security and preservation of the shared data's privacy, they use access control based on RBAC, with the use of Ciphertext-Policy Attributed-based Encryption (CP-ABE) in the process. In this article (Yang et al. 2015), the authors have developed policies to preserve patient privacy, thus making it possible to achieve interoperability of EHRs based on XDS.b and BPPC profiles. EHRs are classified according to the level of privacy based on their sensitivity. Each EHR category uses privacy policies according to the user's consent. The exchange of information is done through XML, and the integration is done through the HL7 standard. The Access Control Management Module represents the business rule of access control. Consequently, controlling the right of access to documents. This work (Abomhara et al. 2018) extends work-based access control (WBAC) in a risk assessment framework targeting EHRs. It mitigates the possibilities of disclosing information that may violate users' privacy who use these systems. The authors (Shahnaz et al. 2019) propose a framework that can be used on EHR systems using blockchain technology. The main focus of the article is the use of blockchain to provide security and privacy, as well as providing storage of electronic records defined on access rules. Meanwhile, the authors (Zaabar et al. 2021) develop the HealthBlock is a blockchain-based system for a decentralized health management system. The system uses blockchain technology integrated into healthcare to create efficient and secure remote patient monitoring (RPM) and EHR management. The presented system's architecture is derived from exploring the concept of decentralized storage and an authorized blockchain network as an access control mechanism to monitor patient vital signs data. A blockchain is used to effectively implement the proposed architecture because it maintains access control only for specific participants who will grant access to the data. In this work, (Lu and Sinnott 2016) propose a semantic methods XACML (eXtensible Access Control Markup Language) model provides access to personal information authorizing access to confidential enforcement of privacy protection policies.

Emergency access

Laws state that access to private patient data must be possible without express authorization from patients, since in emergencies or life-threatening situations, systems must be able to allow such access on an emergency basis. However, EHR systems must provide an option for medical personnel to access user data in an emergency, especially when the user cannot manually grant access to the data. This technique is also known as Break-the-Glass (BTG) (Jayabalan and O'Daniel 2017). Thus, this paper (Eom and Lee 2016) proposes patient-controlled attribute-based encryption (PC-ABE), which allows the user to control access to their health data. This method allows the users to have total control over the data, and whether they can authorize access to it. In emergencies, the victim is unconscious and cannot access their personal health information (PHI). An access key is created that will allow the emergency team to access the user's private data. However, it will only work for that patient. To avoid unauthorized data access after the service's end, the key is granted for a limited time.

De-Identification

Unlike HIPAA, GDPR does not have specific methods for "de-identify" data. Instead, the regulation states that data can be "anonymized" or "pseudonymized" (Medicine 2018). De-identification is a technique that allows certain information to be removed so that it is no longer possible to identify the user. HIPAA requires 18 types of identification to be removed (HIPAA 2013b). Thus, several techniques have been proposed for this purpose. The author (Sun et al. 2018) proposes a signature design based on a decentralized attribute for healthcare blockchain. As a result, the DABE (Distributed Attribute-Based Encryption) scheme for releasing attributes and private keys between organizations. In this technique, they use attributes as a way of identifying the patients, thus hiding the user's real identity, making the data anonymous. The authors (Poulis et al. 2017) present the anonymity method, which permits third parties to access patients' information without disclosing the patient's personal data. The methods that make use of anonymity are increasingly present in the articles since they are ways to provide privacy to users, omitting their information, especially where there is an exchange of information between providers such as hospitals and other institutions related to the health domain. Thus, we can cite (Jayabalan and Rana 2018). This article introduces technicians based on the Publication of Privacy Preservation Data (PPPD) that can be applied to make anonymity before publishing patient information in the insights. The main objective is to ensure that malicious users cannot extract information about any particular individual in the published dataset. Anonymity is a technique that irreversibly modifies data so that user data are no longer directly or indirectly identifiable. This is a technique applied to quasi-identifiers (identifiers that, when combined, provide personally identifiable information) to generalize, hide, and mask the relevant information to be preserved. Hence, several methods can apply, such as generalization, suppression, bucketing, slicing, and randomization. Anonymity is the usual address in healthcare to preserve patient privacy. The process of de-identification and re-identification of data can be accomplished through removal techniques and direct identifiers, such as name, phone numbers, e-mail addresses, and other unique identifiers. Pseudonymization, where names and other information directly identify an individual, is replaced by symbols or other characters. Thus, the de-identification of indirect identifiers where methods include "Suppression," "Generalization," "Disturbance," "Swapping," "Sub-Sampling," and "Masking". Besides, sensitive information can be suppressed with an asterisk, and some other information can be hidden.

Audit

Information systems must be able to provide a level of audit controls, such as access reports. These controls are useful for recording and making it possible to consult the records in order to identify possible improper access to patient data. As well, such records must be reviewed frequently. An institution should consider its risk analysis and organizational factors, such as current technical infrastructure, hardware, and software security features, to determine reasonable and appropriate auditing, as well as controls for information systems that contain or use PHI. HIPAA and ONC specify that auditors' controls are required for healthcare systems (Farhadi et al. 2019). Thus, (Ibrahim and Singhal 2016a) proposes an architecture for information exchange between physicians in different healthcare providers, hence, allowing them to exchange information using cryptography ways to assure users' security and preserve privacy. Besides that, the audit system allows for proper maintenance of transactions and records all information that enters or leaves what has been requested by health providers.

Integrity

Integrity is defined as a security rule in order to protect data from unauthorized alteration or destruction. The reason for this standard is to establish and implement policies and procedures to protect PHI from being compromised, regardless of the source. This will help prevent employees from making accidental or intentional changes and thereby altering or destroying PHI. It can also help prevent changes caused by errors or failures of electronic media. Integrity can be achieved through encryption techniques; many articles present solutions to achieve this requirement, such as (Sharma and Balamurugan 2020), who propose a system to make EHR more secure and at the same time provide a level of privacy. For this, they used blockchain technology using their cryptographic techniques and decentralization. In this paper, we propose a biometric-based blockchain EHR system (BBEHR) blockchain-based framework for the storage and support of EHRs. Also, based on a blockchain network, the patient is able to have exclusive control over his or her data. In addition, each patient has a unique Ethereum (public blockchain platform considered to be the most advanced to code and process smart contracts) address and identifier using smart contracts, making it an arduous task for an unauthorized user to access. Moreover, several types of contracts were used to provide greater data protection, enabling the preservation of privacy (Vora et al. 2018).

Secure transmission

It is necessary to implement measures and techniques to protect against unauthorized access to the information transmitted over a data network. The health provider should implement technical security measures to protect against unauthorized access. Health information must be protected when it is being transmitted over a communications network. Therefore, the institution must analyze these risks and understand the current method used to transmit PHI. Once these methods are reviewed, the entity can determine the best way to protect PHI. In this article (Ismail and Materwala 2020), the authors propose a blockchain framework aimed at EHR (BlockHR). The proposed framework allows patients to transmit their health data through an external network, allowing doctors to support patients by offering a better prognosis, diagnosis, and monitoring. The guarantee of privacy is offered by the blockchain network that makes use of cryptographic means as a way to guarantee the privacy of the information that is being transmitted. On the other hand,(Kho et al. 2015) implemented a DCIFIRHD software application that creates a secure, seamless, and preserves the privacy of electronic health record (EHR) transmission data among various locations in a large metropolitan area in the United States for use in clinical research. The authors developed an application that performs cleaning, pre-processing, and hashing of standardized patient identifier data to remove all protected health information. The application creates combinations of hash codes propagated from patient identifiers using an SHA-512 algorithm compliant with the Health Insurance Portability Act (HIPAA).

Authentication

Authentication refers to the methods that the user can access the EHR system, whether through passwords, PINs, smart cards, tokens, or keys. This article (Al Baqari and Barka 2020) proposes a biometric blockchain EHR system to guarantee the safety exchange and synchronization of EHRs between healthcare providers. Besides, proposing safe access control for the restoration of EHRs is provided to users. The authors propose a solution using biometrics as forms of identification within a blockchain network based on EHRs. According to the HIPAA requirement, the proposed solution that maintaining the patient's identity ensures a single mapping between patients to their respective EHRs, access control to the EHR while providing anonymization of patient data stored within EHR. Whereas, this article (Mamun and Rana 2017) proposes a framework for authentication and a hybrid model for PCEHR access control to provide security and privacy of patients' eHRs using a cryptographic technique. For this, the proposed authentication model uses multichannel authentication and incorporates context restriction with conventional access control models. The central framework employs encryption to update and store EHR data.

Consent

The GDPR and LGPD allow the use of data related to the patient's health as long as the user's explicit consent is given. The user must be clearly informed of how his data will be used. HIPAA enables the use or disclosure of PHI with individual authorization, which must include a number of required elements. Thus, this article (Zhang et al. 2016) presents a proposal for a framework for electronic health record systems permitting data (encrypted for privacy preservation). The proposal is an access control mechanism through consent to enable the exchange of information. Hence, the data requesters must ask users for permission to access the data. To perform this task, they use a conditional proxy re-encryption algorithm, by which the data center re-encrypts the encrypted data without revealing its plain text. Additionally, mutual authentication is achieved using the recipient's public key in the encryption algorithm.

Encryption and decryption

HIPAA specifies that it must implement a mechanism to encrypt and decrypt electronically protected health information. It implies using an algorithmic process to convert data into a form in which there is a low probability of attributing meaning without using a secret key or process (HIPAA 2013b). This article (Guo et al. 2018) performs a study on preserving patient privacy in an EHRs system on the blockchain. Furthermore, it carried out access control based on an attribute-based signature (MA-ABS) scheme with many authorities. The authors propose a symmetric key generation method that simultaneously generates a symmetric session key at two distinct healthcare providers based on existing patients' credentials (Ibrahim and Singhal 2016b). In this article, (Huang et al. 2019) introduced MedBloc, a shared blockchain-based EHR system, through the use of smart contracts and cryptography techniques. It allows patients and healthcare providers to access and, at the same time, share health records in a usable manner while preserving privacy. This article (Xu et al. 2019) presents a new approach to ensure user privacy by preserving the revocable ciphertext policy attribute-based encryption (PR-CP-ABE) scheme, enabling users to revoke privileges and protect privacy immediately. This article (Essa et al. 2019) proposes a new approach to data security in IFDDS healthcare environments using encryption algorithms distributed between different platforms in the cloud. The main objective is to protect sensitive data stored in the cloud, with the least possible impact on latency and performance. IFHDS uses the concept of classification encryption to minimize processing time and encrypt data based on the level of sensitivity. At the same time, IFHDS proposes splitting sensitive data into different parts according to the sensitivity level. The division of this data based on the sensitivity level prevents the cloud storage provider from breaking the data's complete record if it can decrypt part of the data. In addition, Apache Hadoop and Spark allow IFHDS to encrypt and decrypt data and use hardware resources using parallel processing. In addition, Spark masks sensitive data based on the GDPR requirements stored in the EHR.

Automatic logoff

As a practice within institutions, EHR systems should be able to log off users who are accessing the system when they are no longer using the system, thus preventing unauthorized people from accessing confidential patient information, thus exposing private patient information (HIPAA 2013a). Automatic logoff is an effective way to prevent unauthorized users from accessing PHI on a workstation when left unattended for a period. However, in our research, the solutions found do not present information if the systems have automatic logoff capability, so we have not entered any proposal that offers this type of security and privacy requirement.

Discussion

The important features included in the systematic mapping studies are summarized and discussed below. In this section, we will provide the answers to our questions from Section 2:

Privacy challenges in EHR

The advantages of healthcare systems have been considered in recent decades. However, due to its many challenges, the conventional use of the healthcare system is still at an initial step. Perception security and privacy issues are the main concerns and challenges of the e-health system and, consequently, EHR systems. The principle that regulates the doctor–patient relationship is seen as privacy. Patients are required to share the necessary information with their physicians. However, they may refuse to reveal important information, as disclosing some information can result in social disapproval and discrimination (Ghazvini and Shukur 2013).

Nevertheless, it is essential to comprehend how well electronic health records (EHR) are protected and the main factors that can lead to a successful EHR. Over time, EHR gathers personal information that is significant to a person's life and social status.

Encrypted methods are becoming increasingly common as a way to preserve data and offer privacy. However, the encryption method is not entirely secure. The computational cost of encryption can be high for EHR systems or low-capacity equipment such as health trackers, IoT devices, and smart watches, which are being used by patients to monitor daily activities and measure personal data, such as blood pressure, heart rate, and electrocardiograms (ECG). The activity log can also reveal user behavior and identity due to the account's fixed address. In addition, to resist malicious attacks (e.g., statistical attacks), healthcare systems have to change the encryption keys periodically. Thus, this entails a cost of storage and management of these keys' key holders, which will be necessary to decrypt in the future (Guo et al. 2018). Meanwhile, recent advances in the exploration and storage of a large volume of data without compromising privacy have become a significant challenge for researchers (Jayabalan and Rana 2018) and (Essa et al. 2019).

The use of blockchain as a solution for security and privacy has become increasingly common in solutions for EHR systems. As well, smart contracts have become a trend as a form of access control due to their decentralized form that is characteristic of this technology associated with cryptography. The challenges associated with blockchain are related to data storage on the blockchain network, causing confidentiality and scalability problems. Thus, data on a blockchain network is visible to everyone in the blockchain chain. The data may contain private user data, test results, history, or other reports. We can also mention other defaults, such as a lack of social skills due to the lack of understanding about blockchain technology is understandable only by a few people. We can also mention the lack of a universal standard that defines the network patterns (Shahnaz et al. 2019). On the other hand, sharing EHR information can lead to challenges for users in knowing who has access to their data. In a real scenario, some healthcare providers may have access to the data and use it illegally, leading to a privacy problem. This is also due to the fact that the sharing of EHRs on the blockchain has not been investigated in real-world scenarios (Nguyen et al. 2019).

The human factor needs to be taken into account; training employees and at the same time enabling them to deal with sensitive data is something fundamental, like investing in technologies and computational means to assure the privacy and security of information (Smaradottir 2018).

The main requirements identified in EHRs

EHRs, like any other system, need minimum requirements, such as access control and authentication mechanisms; these requirements are the most cited in the researched articles. However, EHR is responsible for handling and storing sensitive patient information, such as medications, progress reports, vital signs, medical histories, immunization reports, laboratory data, and radiology reports. Thus, other precautions must be taken to avoid losing the privacy of the information in these systems. In addition, ensuring data integrity is vital for these EHRs; for this reason, encryption techniques are cited continuously in almost all articles. We

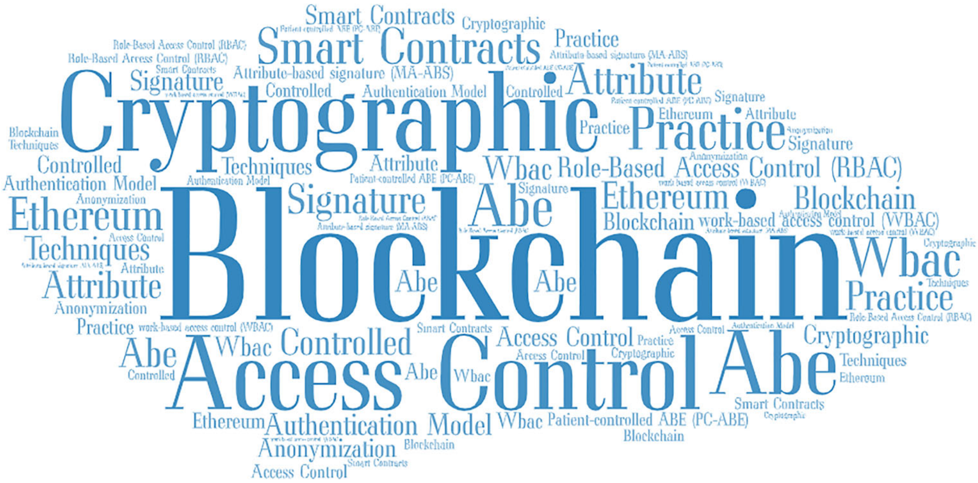


Fig. 7 Wordcloud with the selected main techniques to provide privacy

can also highlight audit mechanisms that are essential for tracking, thus making it possible to carry out periodic consultations on patient records, identifying whether the people who are accessing patient data are really who should access it.

Laws and policies constantly cite other means that guarantee the information's privacy as techniques that allow the de-identification of information. A common requirement when analyzing laws such as GDPR and LGPD is that the user has the possibility that their information will be deleted when the purpose of storing that information ends, as well as authorizing the use of personal data and that the user has full consent for how their information will be used.

The main published techniques regarding privacy in EHRs

We can highlight that there is a concern with the development of techniques as a way of providing confidentiality and data integrity (Ibrahim and Singhal 2016b), (Lu and Sinnott 2016; Guo et al. 2018), and (Essa et al. 2019). Simultaneously, it was realized that there are enough solutions concerned with anonymization (Sun et al. 2018) and pseudonymization (Jayabalan and Rana 2018) of data as a way of preserving users' privacy, as required by HIPAA (HIPAA 2013a) and GDPR (GDPR 2016). Meanwhile, the use of access control techniques that make use of cryptographic means have become a trend, and with the use of smart contracts for this purpose, it has become increasingly common (Sun et al. 2018) and (Vora et al. 2018). Other requirements such as emergency access, required in EHR systems, are less implemented, as well as the use of consent to access users' private data, whereas techniques such as secure transmission were also little explored since there is a significant demand to ensure this data's privacy and security between healthcare providers and other intuitions that need to receive this information. However, our most prominent highlight is the large number of articles that are unaware of the laws and standards that regulate how to provide data privacy in EHR systems. Many articles do not quote common laws or policy or even formalize their techniques based on required requirements.

Figure 7 presents a wordcloud with all the methods found in the searches cited in the researched articles on preserving privacy. In this wordcloud, the method name's font size varies according to the number of times that the technique was cited in the analyzed articles (thus, names with large fonts represent the method that appears in more quantity). Hence, this wordcloud is useful for highlighting the most prominent methods within our systematic mapping scope.

The main published techniques that meet the requirements

We can see that the selected articles propose solutions for the security and preservation of data privacy in EHR systems. Hence, almost all of them are made up of one or more requirements, fewer requirements like automatic logoff that were not mentioned. Some articles like (Ibrahim and Singhal 2016a; Guo et al. 2018; Sun et al. 2018) have several requirements in their approaches. In addition, access control, integrity, and encryption solutions are present in almost everyone. The laws and policies specify that these requirements are essential and vital to provide security and preserve users' data privacy. However, some articles focus more on a requirement, just like (Poulis et al. 2017) and (Jayabalan and Rana 2018). Requirements such as user consent as required by laws such as GDPR and LGPD have only been found in two articles, (Verdonck and Poels 2020), and (Zhang et al. 2016).

Conclusions

This work presented a systematic mapping of privacy in electronic health record research. The research collected 848 papers between October 16 and 14 of November 2021 and was carried out in the base Scopus (Elsevier). After applying the inclusion and exclusion criteria, the analysis of the papers was carried out in 30 works resulting in the following conclusions.

Preserving user data privacy is extremely important in healthcare environments. The main privacy challenges related to EHR systems consist of increasing data privacy without compromising the performance and interoperability of these systems. Blockchain has been used in many EHR systems as a solution to achieve data privacy. However, it is a challenge to maintain traceability by recording metadata that can be mapped to private data of the users applying a particular mapping function that can be hosted outside the blockchain. Therefore, the right to be forgotten must be applied by eliminating the link between the blockchain and private data in the mapping occupation. Besides, the analyzed works showed a growing interest in privacy in electronic health record research in the last 6 years.

The main law requirements that EHR systems must respect are encryption techniques, access control, integrity, audit controls, followed by de-identification, emergency access, consent, secure transmission, authentication, and automatic logoff. When considering systems that need to provide privacy and security to user data, those concerns must be considered from the beginning and throughout the system development life cycle.

Our research noticed that the majority of articles do not bring all the requirements in their approach. Thus, most articles focus on just a few requirements such as access control, data integrity, data security transmission, data encryption, and decryption. The works are not entirely based on personal health information protection laws and policies such as data emergency access strategies, user consent, audit control, and automatic logoff. Furthermore, the authors do not mention in detail or list their proposed solution on which system features comply with laws or policies. Thus, the lack of a systematic approach between EHR solutions and existing laws or policies leads to better strategies for developing a certification process for EHR systems.

The lack of standardization for the development of EHR systems has been seen as one of the main problems, and developers do not have a reference guide to analyze the privacy and security requirements that EHR systems must meet. Therefore, a set of rules that could be used to guide the developer on what privacy and security requirements EHR systems must meet would be vitally important to guide the development of more secure EHR systems. At the same time, a set of rules that could certify these systems in terms of privacy and security would be extremely important for EHR systems.

Author Contributions All authors contributed equally to this work.

Funding Open access funding provided by FCT—FCCN (b-on). The author(s) received no financial support for the research, authorship, and/or publication of this article.

Declarations

Competing interests The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed consent The authors declare that this research does not contain any individual person's data in any form (including any individual details, images or videos).

References

Abomhara M., Køien G. M., Oleshchuk V. A., Hamid M. (2018) Towards risk-aware access control framework for healthcare information sharing. In: Proceedings of the 4th International Conference on Information Systems Security and Privacy - 1, ICISSP, INSTICC, SciTePress, pp. 312–321. https://doi.org/10.5220/0006608103120321

Ahmadian L., Khajouei R. (2012) Impact of computerized order sets on practitioner performance. Quality of Life through Quality of Information, 1129–1131

Ahmadian L., Salehi Nejad S., Khajouei R. (2015) Evaluation methods used on health information systems (hiss) in Iran and the effects of hiss on Iranian healthcare: A systematic review. International Journal of Medical Informatics, 84. https://doi.org/10.1016/j.ijmedinf.2015.02.002

Al Baqari M., Barka E. (2020) Biometric-based blockchain EHR system (BBEHR). In: 2020 International Wireless Communications and Mobile Computing (IWCMC), pp. 2228–2234, https://doi.org/10.1109/IWCMC48107.2020.9148357

Al-Issa Y., Ottom M. A., Tamrawi A. (2019) eHealth cloud security challenges: A survey. Journal of Healthcare Engineering 2019:7516035 https://doi.org/10.1155/2019/7516035

Alanazi H. O., Zaidan A. A., Zaidan B. B., Kiah M. L., Al-Bakri S. H. (2015) Meeting the security requirements of electronic medical records in the era of high-speed computing. J Med Syst 39(1):165

Aldossary S., Allen W. (2016) Data security, privacy, availability and integrity in cloud computing: Issues and current solutions. Int. J. Adv. Comput. Sci. Appl. 7, https://doi.org/10.14569/IJACSA.2016.070464

Amato F., De Pietro G., Esposito M., Mazzocca N. (2015) An integrated framework for securing semi-structured health records. Knowl.-Based Syst. 79:99–117. https://doi.org/10.1016/j.knosys.2015.02.004

Aslam U., Sohail A., Aziz H. I. T., Vistro M. (2019) The importance of preserving the anonymity in healthcare data: a survey. International Journal Of Scientific & Technology Research 8(11), NOVEMBER 2019

Balsari S., Fortenko A., Blaya J. A., Gropper A., Jayaram M., Matthan R., Sahasranam R., Shankar M., Sarbadhikari S. N., Bierer B. E., Mandl K. D., Mehendale S., Khanna T. (2018) Reimagining health data exchange: an application programming interface–enabled roadmap for India. J Med Internet Res 20(7):e10725. https://doi.org/10.2196/10725

Berner E. S., Detmer D. E., Simborg D. (2005) Will the wave finally break? A brief view of the adoption of electronic medical records in the United States. J. Am. Med. Inform. Assoc. 12(1):3–7. https://doi.org/10.1197/jamia.M1664

Cifuentes M., Davis M., Fernald D., Gunn R., Dickinson P., Cohen D. J. (2015) Electronic health record challenges, workarounds, and solutions observed in practices integrating behavioral health and primary care. The Journal of the American Board of Family Medicine 28(Supplement 1):S63–S72. https://doi.org/10.3122/jabfm.2015.S1.150133

Dybå T, Dingsøyr T (2008) Empirical studies of agile software development: A systematic review. Inf. Softw. Technol. 50:833–859. https://doi.org/10.1016/j.infsof.2008.01.006

Edemacu K., Park H. K., Jang B., Kim J. W. (2019) Privacy provision in collaborative eHealth with attribute-based encryption: survey, challenges and future directions. IEEE Access 7:89614–89636. https://doi.org/10.1109/ACCESS.2019.2925390

Eom J., Lee K. (2016) Patient-controlled attribute-based encryption for secure electronic health records system. J. Med. Syst. 40:253. https://doi.org/10.1007/s10916-016-0621-3

Essa Y. M., Hemdan E. E. D., El-Mahalawy A., Attiya G., El-Sayed A. (2019) IFHDS: Intelligent framework for securing healthcare bigdata. J. Med. Syst. 43(5):124. https://doi.org/10.1007/s10916-019-1250-4

Farhadi M., Haddad H., Shahriar H. (2019) Compliance checking of open source EHR applications for HIPAA and ONC security and privacy requirements. In: 2019 IEEE 43rd annual computer software and applications conference (COMPSAC) vol. 1, pp. 704–713. https://doi.org/10.1109/COMPSAC.2019.00106

Fernández-Alemán J. L., Señor I. C., Ángel Oliver Lozoya P., Toval A. (2013) Security and privacy in electronic health records: a systematic literature review. J. Biomed. Inform. 46(3):541–562. https://doi.org/10.1016/j.jbi.2012.12.003

Gardiyawasam Pussewalage H. S., Oleshchuk V. A. (2016) Privacy preserving mechanisms for enforcing security and privacy requirements in e-health solutions. Int. J. Inf. Manag. 36(6, Part B):1161–1173. https://doi.org/10.1016/j.ijinfomgt.2016.07.006

GDPR (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (General Data Protection Regulation). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Ghazvini A., Shukur Z. (2013) Security challenges and success factors of electronic healthcare system. Procedia Technol. 11:212–219. 4th International Conference on Electrical Engineering and Informatics, ICEEI 2013. https://doi.org/10.1016/j.protcy.2013.12.183

Gkoulalas-Divanis A., Loukides G., Sun J. (2014) Publishing data from electronic health records while preserving privacy: A survey of algorithms. J. Biomed. Inform. 50:4–19. https://doi.org/10.1016/j.jbi.2014.06.002, special Issue on Informatics Methods in Medical Privacy

Grana M., Jackwoski K. (2015) Electronic health record: a review. In: 2015 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), IEEE Computer Society, Los Alamitos, CA, USA, pp. 1375–1382. https://doi.org/10.1109/BIBM.2015.7359879

Guo R., Shi H., Zhao Q., Zheng D. (2018) Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access 6:11676–11686. https://doi.org/10.1109/ACCESS.2018.2801266

Hakim S. A., Sensuse D. I. (2018) Knowledge mapping system implementation in knowledge management: A systematic literature review. In: 2018 International Conference on Information Management and Technology (ICIMTech), pp. 131–136 https://doi.org/10.1109/ICIMTech.2018.8528190

Hathaliya J. J., Tanwar S., Evans R. (2020) Securing electronic healthcare records: a mobile-based biometric authentication approach. Journal of Information Security and Applications 102528:53. https://doi.org/10.1016/j.jisa.2020.102528

HIPAA (2013a) HIPAA survival guide HITECH act summary - HIPAA Privacy Rule 164.506. http://www.hipaasurvivalguide.com/hipaa-regulations/164-506_BAK_01202013.php

HIPAA (2013b) Summary of the HIPAA Privacy Rule. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

HITECH (2009) Health information technology for economic and clinical health (HITECH) act. http://www.hhs.gov/hipaa/for-professionals/specialtopics/HITECH-act-enforcement-interim-final-rule/, last Accessed 16 September 2020

Horodyski D. (2015) 2013 OECD Guidelines on the protection of privacy and transborder flows of personal data as an example of recent trends in personal data protection, ResearchGate, pp. 255–266, https://doi.org/10.13140/RG.2.1.1508.4405

Hu V., Ferraiolo D., Kuhn D., Schnitzer A., Sandlin K., Miller R., Scarfone K. (2014) Guide to attribute based access control (ABAC) definition and considerations. National Institute of Standards and Technology Special Publication, 162–800

Huang J., Qi Y. W., Asghar M. R., Meads A., Tu Y. (2019) MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data. In: 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 594–601, https://doi.org/10.1109/TrustCom/BigDataSE.2019.00085

Hussien H. M., Yasin S. M., Udzir S. N. I., Zaidan A. A., Zaidan B. B. (2019) A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. J. Med. Syst. 43(10):320. https://doi.org/10.1007/s10916-019-1445-8

Häyrinen K., Saranto K., Nykänen P. (2008) Definition, structure, content, use and impacts of electronic health records: a review of the research literature. Int. J. Med. Informatics 77(5):291–304. https://doi.org/10.1016/j.ijmedinf.2007.09.001

Ibrahim A., Singhal M. (2016a) An abstract architecture design for medical information exchange. In: 2016 International Conference on Industrial Informatics and Computer Systems (CIICS), pp. 1–6 https://doi.org/10.1109/ICCSII.2016.7462427

Ibrahim A., Singhal M. (2016b) A simultaneous key generation technique for health information exchange (hie) based on existing patients' credentials

Ismail L., Materwala H. (2020) BlockHR: A blockchain-based framework for health records management. In: Proceedings of the 12th International Conference on Computer Modeling and Simulation, Association for Computing Machinery, New York, NY, USA, ICCMS '20, p 164–168 https://doi.org/10.1145/3408066.3408106

Jagtap S. T., Thakar C. M., El imraniO, Phasinam K., Garg S., Ventayen R. J. M. (2021) A framework for secure healthcare system using blockchain and smart contracts. In: 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 922–926 https://doi.org/10.1109/ICESC51422.2021.9532644

Jayabalan M., O'Daniel T. (2017) Continuous and transparent access control framework for electronic health records: A preliminary study. In: 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), pp. 165–170 https://doi.org/10.1109/ICITISEE.2017.8285487

Jayabalan M., Rana M. E. (2018) Anonymizing healthcare records: A study of privacy preserving data publishing techniques. Adv. Sci. Lett. 24:1694–1697. https://doi.org/10.1166/asl.2018.11139

Kadhim K. T., Alsahlany A. M., Wadi S. M., Kadhum H. T. (2020) An overview of patient's health status monitoring system based on Internet of Things (IoT). Wireless Pers. Commun. 114(3):2235–2262. https://doi.org/10.1007/s11277-020-07474-0

Kanwal T., Anjum A., Khan A. (2020) Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. Cluster Computing https://doi.org/10.1007/s10586-020-03106-1

Kayaalp M. (2018) Patient privacy in the era of big data. Balkan Med. J. 35(1):8–17. https://doi.org/10.4274/balkanmedj.2017.0966 28903886[pmid]

Keshta I., Odeh A. (2020) Security and privacy of electronic health records. Concerns and challenges. Egyptian Informatics Journal. https://doi.org/10.1016/j.eij.2020.07.003

Kho A. N., Cashy J. P., Jackson K. L., Pah A. R., Goel S., Boehnke J., Humphries J. E., Kominers S. D., Hota B. N., Sims S. A., Malin B. A., French D. D., Walunas T. L., Meltzer D. O., Kaleba E. O., Jones R. C., Galanter W. L. (2015) Design and implementation of a privacy preserving electronic health record linkage tool in Chicago. J. Am. Med. Inform. Assoc. 22(5):1072–1080. https://doi.org/10.1093/jamia/ocv038

Kitchenham B. (2004) Procedures for performing systematic reviews. Keele, UK, Keele Univ, 33

Kloss L. L., Brodnik M. S., Rinehart-Thompson L. A. (2018) Access And disclosure of personal health information: A challenging privacy landscape in 2016-2018. Yearb Med Inform 060(01):060–066

Lu Y., Sinnott R. O. (2016) Semantic-based privacy protection of electronic health records for collaborative research. In: 2016 IEEE Trustcom/BigDataSE/ISPA, pp. 519–526, https://doi.org/10.1109/TrustCom.2016.0105

Mamun Q., Rana M. (2017) A robust authentication model using multi-channel communication for eHealth systems to enhance privacy and security. In: 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 255–260 https://doi.org/10.1109/IEMCON.2017.8117210

Medicine J. H. (2018) Preparing for the EU GDPR In research settings guidance. https://www.jhsph.edu/offices-and-services/institutional-review-board/

Mehndiratta P., Sachdeva S., Kulshrestha S. (2014) A model of privacy and security for electronic health records. In: Madaan A., Kikuchi S., Bhalla S. (eds) Databases in Networked Information Systems, Springer International Publishing, Cham, pp. 202?213

Nguyen D. C., Pathirana P. N., Ding M., Seneviratne A. (2019) Blockchain for secure EHRs sharing of mobile cloud based e-health systems, vol 7

Nortey R. N., Yue L., Agdedanu PR, Adjeisah M (2019) Privacy module for distributed electronic health records (EHRs) using the blockchain. In: 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA), pp. 369–374 https://doi.org/10.1109/ICBDA.2019.8713188

Nweke L., Yeng P., Wolthusen S., Yang B. (2020) Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices. Int. J. Adv. Comput. Sci. Appl. 11:683–690. https://doi.org/10.14569/IJACSA.2020.0110286

Odeh A., Keshta I., Aboshgifa A., Abdelfattah E. (2022) Privacy and security in mobile health technologies: Challenges and concerns. In: 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0065–0071 https://doi.org/10.1109/CCWC54503.2022.9720863

Pai M. M. M., Ganiga R., Pai R. M., Sinha R. K. (2021) Standard electronic health record (EHR) framework for Indian healthcare system. Health Serv. Outcomes Res. Method. 21(3):339–362. https://doi.org/10.1007/s10742-020-00238-0

Petersen K., Feldt R., Mujtaba S., Mattsson M. (2008) Systematic mapping studies in software engineering. In: EASE

Petersen K., Vakkalanka S., Kuzniarz L. (2015) Guidelines for conducting systematic mapping studies in software engineering: An update. Inf. Softw. Technol. 64:1–18. https://doi.org/10.1016/j.infsof.2015.03.007

Poulis G., Loukides G., Skiadopoulos S., Gkoulalas-Divanis A. (2017) Anonymizing datasets with demographics and diagnosis codes in the presence of utility constraints. J. Biomed. Inform. 65:76–96. https://doi.org/10.1016/j.jbi.2016.11.001

Pramanik P. K. D., Pal S., Mukhopadhyay M. (2019) Healthcare Big Data: A Comprehensive Overview, IGI Global, Hershey, PA, USA, pp. 72–100. Intelligent Systems for Healthcare Management and Delivery https://doi.org/10.4018/978-1-5225-7071-4.ch004

Rana M. E., Jayabalan M. (2016) Privacy preserving anonymization techniques for patient data: An overview. In: Conference: 3rd International Conference on Knowledge, Information and Software Engineering (ICKIS2016)

Rezaeibagha F., Mu Y. (2016) Distributed clinical data sharing via dynamic access-control policy transformation. Int. J. Med. Informatics 89:25–31. https://doi.org/10.1016/j.ijmedinf.2016.02.002

Richter G., Borzikowsky C., Lieb W., Schreiber S., Krawczak M., Buyx A. (2019) Patient views on research use of clinical data without consent: legal, but also acceptable? European Journal of Human Genetics : EJHG 27(6):841–847. https://doi.org/10.1038/s41431-019-0340-6 30683927 [pmid]

Scholl M. A., Stine K. M., Hash J., Bowen P., Johnson L. A., Smith C. D., Steinberg D. I. (2008) SP 800-66 Rev. 1. an introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule, national institute of standards & technology, Gaithersburg, MD, USA, chap, 1

Shah S. M., Khan R. A. (2020) Secondary use of electronic health record: Opportunities and challenges. IEEE Access 8:136947–136965. https://doi.org/10.1109/ACCESS.2020.3011099

Shahnaz A., Qamar U., Khalid A. (2019) Using blockchain for electronic health records. IEEE Access 7:147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373

Sharma Y., Balamurugan B. (2020) Preserving the privacy of electronic health records using blockchain. Procedia Computer Science 173:171–180. https://doi.org/10.1016/j.procs.2020.06.021, international Conference on Smart Sustainable Intelligent Computing and Applications under ICITETM2020

Shrestha N. M., Alsadoon A., Prasad P. W. C., Hourany L., Elchouemi A. (2016) Enhanced e-health framework for security and privacy in healthcare system. In: 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC), pp. 75–79 https://doi.org/10.1109/ICDIPC.2016.7470795

Sittig D., Singh H. (2010) A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. Quality & Safety in Health Care 19 Suppl 3:i68–74. https://doi.org/10.1136/qshc.2010.042085

Smaradottir B. F. (2018) Security management in electronic health records: Attitudes and experiences among health care professionals. In: 2018 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 715–719 https://doi.org/10.1109/CSCI46756.2018.00143

Sun Y., Zhang R., Wang X., Gao K., Liu L. (2018) A decentralizing attribute-based signature for healthcare blockchain. In: 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1–9 https://doi.org/10.1109/ICCCN.2018.8487349

Tan J. (2008) Healthcare information systems and informatics: Research and Practices: Research and Practices. IGI Global

Tasatanattakool P., Chian T. (2017) User authentication algorithm with role-based access control for electronic health systems to prevent abuse of patient privacy. In: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), pp. 1019–1024 https://doi.org/10.1109/CompComm.2017.8322697

Verdonck M., Poels G. (2020) Architecture and value analysis of a blockchain-based electronic health record permission management system (short paper). In: VMBO

Vora J., Nayyar A., Tanwar S., Tyagi S., Kumar N., Obaidat M. S., Rodrigues J. J. P. C. (2018) Bheem: A blockchain-based framework for securing electronic health records. In: 2018 IEEE Globecom Workshops (GC Wkshps), pp. 1–6 https://doi.org/10.1109/GLOCOMW.2018.8644088

Wazid M., Das A. K., Kumar N., Conti M., Vasilakos A. V., Wazid M., Das A. K., Kumar N., Conti M., Vasilakos A. V. (2018) A Novel Authentication and Key Agreement Scheme for Implantable Medical Devices Deployment. IEEE J Biomed Health Inform 22(4):1299–1309

Xu R., Joshi J., Krishnamurthy P. (2019) An integrated privacy preserving attribute based access control framework supporting secure deduplication. IEEE Transactions on Dependable and Secure Computing, 1–1. https://doi.org/10.1109/TDSC.2019.2946073

Yang C., Liu C., Tseng T. (2015) Design and implementation of a privacy aware framework for sharing electronic health records. In: 2015 International Conference on Healthcare Informatics, pp. 504–508 https://doi.org/10.1109/ICHI.2015.92

Yüksel B., Küpçü A., Öznur Ö. (2017) Research issues for privacy and security of electronic health services. Futur. Gener. Comput. Syst. 68:1–13. https://doi.org/10.1016/j.future.2016.08.011

Zaabar B., Cheikhrouhou O., Jamil F., Ammi M., Abid M. (2021) Healthblock: A secure blockchain-based healthcare data management system. Comput. Netw. 200:108500. https://doi.org/10.1016/j.comnet.2021.108500

Zhang A., Bacchus A., Lin X. (2016) Consent-based access control for secure and privacy-preserving health information exchange. Security and Communication Networks 9(16):3496–3508. https://doi.org/10.1002/sec.1556