Informatics in Medicine Unlocked 49 (2024) 101552

Contents lists available at ScienceDirect

Informatics in Medicine Unlocked

journal homepage: www.elsevier.com/locate/imu

Access control solutions in electronic health record systems: A systematic review

Usha Nicole Cobrado [a], Suad Sharief [a], Noven Grace Regahal [a], Erik Zepka [b,c], Minnie Mamauag [a,*], Lemuel Clark Velasco [a,d,**]

[a] Mindanao State University-Iligan Institute of Technology, Iligan City, Philippines
[b] Institute for Science, Technology & Culture, Vancouver, Canada
[c] University of Barcelona, Barcelona, Spain
[d] Premiere Research Institute of Science and Mathematics-Center for Computational Analytics and Modelling, Iligan City, Philippines

ARTICLE INFO

Keywords:
Access control
Electronic health record
Identification
Authentication
Authorization
Accountability
Data privacy
Data security

ABSTRACT

Electronic Health Records (EHRs) are electronically-stored patient medical histories shared among healthcare institutions. Recent studies show that EHRs experience healthcare data protection challenges, and the difficulty lies in providing access to the right individuals at the appropriate time and place. This study synthesizes and analyzes existing literature on access control solutions in EHRs through a systematic literature review. Using the 2020 PRISMA guidelines, a total of 20 qualified journal articles were examined and each proposed mechanism was grouped according to the four categories of access control: Identification, Authentication, Authorization, and Accountability (IAAA). Our findings reveal an interconnection between these categories, with the most popular authorization mechanism being Attribute-based Access Control (ABAC). Methodologies analyzed include a credential system (12 studies), authentication (10 studies), and accountability (2 studies); these most commonly used unique IDs, digital signatures and access control logs respectively. Prominent research gaps found in the sample literature are methodology implementation and standards compliance limitations, of which the former includes the lack of multi-factor authentication, emergency access, patient consent, and accountability. From these findings we infer that further research is needed to protect EHRs from these information security threats.

1. Introduction

The advancement of tools in the healthcare industry is an essential component in improving the quality of patient care management. At the same time, the emergence of health information technology solutions and the increasing number of healthcare institutions embracing digital health has given rise to repositories of sensitive data and information, making them vulnerable to a variety of potential threats [1–4]. Electronic health record systems (EHRs) have gained wide use, replacing paper-based systems and serving as a legally recognized record that is institutionally generated, maintained, and shared across multiple institutions [2]. EHRs are otherwise known as electronic medical records (EMRs) utilized when health data is exchanged among different medical institutions - although the two terms are often used interchangeably [5,6], one primary distinction between an EMR and an EHR is the capacity to communicate entire information in real-time. An EMR collects information from a single care provider and makes it available solely to that care provider. However, EHRs are intended to be utilized by different healthcare practitioners and organizations. It is in this exchange that EHRs commonly experience security issues. These include unauthorized access, information disclosure, loss of authenticity, lack of accountability, data inaccuracies, insecure personal information, data tampering, and exploitation of human vulnerability. This lack of data security is additionally a concern of physicians regarding their patients' records [2,6–12]. It constitutes a significant area of concern to know and ensure who can collect, use, and share patient data when maintaining data integrity and providing effective healthcare treatment. Safeguarding health information's privacy and confidentiality is achieved by incorporating robust security measures within EHRs [13,14]. Numerous existing studies have consistently highlighted the importance of

* Corresponding author.
** Corresponding author. Mindanao State University - Iligan Institute of Technology, Iligan, Lanao del Norte, Philippines.
E-mail addresses: ushanicole.cobrado@g.msuiit.edu.ph (U.N. Cobrado), suad.sharief@g.msuiit.edu.ph (S. Sharief), novengrace.regahal@g.msuiit.edu.ph (N.G. Regahal), xoxlabs@gmail.com (E. Zepka), minnie.mamauag@g.msuiit.edu.ph (M. Mamauag), lemuelclark.velasco@g.msuiit.edu.ph (L.C. Velasco).

https://doi.org/10.1016/j.imu.2024.101552
Received 4 May 2024; Received in revised form 27 June 2024; Accepted 11 July 2024
Available online 15 July 2024

adhering to the Health Insurance Portability and Accountability Act (HIPAA), particularly emphasizing access control as one of the key technical components of HIPAA compliance entailing that it should only permit authenticated and authorized users to access the data [6,9,10,13–18]. In addressing security concerns, each concern is matched with a specific security requirement and solution, with access control being a commonly referenced term [10,19–21]. To this end, we consider access control in EHRs the core security concerns for patients and physicians.

Access control is a security measure that allows data owners to authorize access to users and to determine which of them are allowed to read, execute, share, and modify resources in a system [19,21–24]. In the context of EHRs, access control can be defined as a mechanism that allows authorized users to access patient records while maintaining confidentiality and resource integrity through prevention of unauthorized access [10,19–21,25]. In order to protect health records, the access control to be implemented should cover identification, authentication, authorization, and accountability (IAAA) [26,27]. Identification is the process of determining the identity of a particular user while authentication is the process of proving an identity. Methods include login or sign-in mechanisms, such as usernames and passwords, biometrics, or PINs. Authorization is the concept of determini-ng authorized users in performing certain actions or accessing particular data, such as the access control models themselves. Lastly, accountability or auditing is the act of logging user actions or review, which allows healthcare providers to track unauthorized access. Several access control approaches are being used to tackle access control requirements and to address evolving security concerns [28,29]. These include ones that focus on blockchain technology, cryptography, multi-factor authentication, emergency access, wireless solutions, as well as physical access control which are widely present among wearable devices in the field of healthcare [10,19,22,24,28–30]. Despite extensive research on access control for EHRs, there is no unified solution that satisfies the needs of all healthcare organizations. The challenge lies in the development of an access control solution that will provide the right access to the appropriate people, adapting to the location and time in question.

As represented in the literature, access control is considered an important security measure that aids in creating a security barrier to protect the data contained in a healthcare information system. It has received attention in EHRs that include those in the form of wearable or mobile devices and/or are cloud-based, due to the threats associated with it including malicious attacks, lack of accountability, leakage, unauthorized access, data disclosures, and theft [19–22,24,31,32]. Several access control models and methodologies have been published in the literature. One group of studies proposes solutions that aim to prevent unauthorized disclosure [33,34]. Some studies include methods, techniques, protocols, frameworks, schemes, structures, and models [35–37]. Another group of studies uses methods that partially adhere to privacy requirements [34,38]. Despite the numerous studies, there is a lack of synthesis and analysis in the field. Accordingly, this study seeks to perform such a synthesis, identify research gaps, and derive insights into the different access control mechanisms, requirements, and approaches used for EHRs. The specific objectives of the study are: (1) to screen and profile the literature on access control in EHRs to come up with a sample size that will be used in the systematic review; (2) to conduct a scoping review, methodological analysis, and research gap identification of the solutions discovered. We will follow a systematic review process making use of organized steps of investigation to identify information in the literature that supports new or emerging notions [39] to synthesize and analyze the present access control solutions. The study hopes to benefit developers and systems analysts in having prior knowledge of what requirements should be met to ensure secured access to information in EHRs; these include healthcare providers, medical practitioners, and information technology or information systems researchers concerned with data accuracy, integrity, consistency, proper information, and user management. The study distinguishes frameworks, models, mechanisms, and security compliance in synthesizing access control solutions and insights for future assessment.

The remainder of this review is organized as follows: Section 2 introduces the methodologies and research approaches employed in the study. Section 3 provides an in-depth analysis of the results relating to the different access control solutions among EHRs. Within this section, the researchers also identified prevalent research gaps in the existing literature. Lastly, Section 4 concludes the study and offers recommendations for future research endeavors.

2. Methodology

This literature review aims to compile, evaluate, and assess concepts from various research projects, recognize gaps in the literature, analyze boundaries, and predict potential areas for future research [40–42]. It will utilize a structured process that makes use of organized steps of investigation to identify information in the literature supporting new or emerging concepts and follows the guidelines presented in the 2020 Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA) [24,25,27,39].

The PRISMA Statement includes a 27-item checklist and a four-phase flow diagram. It is a reporting guideline that allows researchers to ensure the validity and transparency in documenting a systematic review [43,44]. The lack of reporting an item from the checklist provides evidence associated with increased risk of bias. The PRISMA guidelines also encourage researchers in locating reliable and accurate sources of information [45]. It also provides clear indication where sufficient information is necessary in appraising the reliability of a review [44].

The PubMed, IEEE, ScienceDirect, Springer Link, MEDLINE, and Google Scholar databases were utilized to consolidate and extract peer-reviewed articles relating to access control solutions in EHRs. These databases were selected after a preliminary examination of several systematic reviews which covered a similar topic. An initial search was conducted to look for these articles and to formulate keywords that must be satisfied by existing studies to be used in the literature review. In the article search, there are 8 keywords identified which include access control, electronic health records, identification, authentication, authorization, accountability, privacy, and security. It is relevant to include this set of keywords to capture the literature centered on the study of access control solutions among EHRs relevant to the topic. The researchers believe that aligning the literature search with the databases with most substantial contents and contribution to the body of knowledge in literature as well as selecting the aforementioned keywords would encapsulate the needed documents to justify the methodologies and contributions this study presents. In addition, the keywords were also derived from the common keywords identified in the literature studies selected [34,46,47] as presented in Table 1.

Table 1
Keywords.

Keywords	Search string
Access control [36,37,46,48–55]	"access control" OR "access management"
Electronic Health Record [33,37,51,56–59]	"electronic health record" OR "electronic health records" OR "EHR" OR "EHR system" OR "electronic medical record" OR "electronic medical records" OR "EMR"
Identification [35,51,53,56]	"identification" OR "identity management"
Authorization [33,37,49,57,59,60]	"authorization" OR "access control model" OR "authorization rule" OR "access control policy" OR "access control policies" OR "role-based access control" OR "RBAC" OR "MAC"
Authentication [50,54,55,61–63]	"authentication" OR "two-factor authentication" OR "multi-factor authentication"
Accountability [46,63]	"accountability" OR "audit" OR "auditing" OR "auditability"
Data Privacy [35,37,48,50,52,54,60,63]	"data privacy" OR "privacy" OR "privacy preservation"
Data Security [33,37,56,64]	"data security" OR "security"

As shown in Fig. 1, the keywords were used to search for articles in the identified databases, which yielded 23,955 results. Duplicate studies were then removed, resulting in 23,464 articles. The selection of studies was limited to articles having a publication year between 2013 and 2023 [25], producing 22,739 results and ensuring that the proposed access control solutions in safeguarding EHRs are aligned with recent requirements and security concerns [24,25,43,65,66]. Ongoing studies were excluded from the sample size, as well as non-English papers [24,25,43,65,66], resulting in 22,489 articles. A total of 4386 studies were removed from the selection as they were not classified as journal articles or conference papers [24,66]. This produced an initial sample size of 18,103 articles, which were further downsized by discarding articles which didn't contain any of the keywords identified in Table 1 in the articles' title, abstract, introduction, and conclusion, as well as studies which didn't focus on access control for EHRs and EMRs specifically. Studies which lacked a full-text view were also excluded from the sample size. Furthermore, articles without an evaluation method, such as security analysis and performance analysis, for the proposed access control solutions were likewise removed. A total of 17,863 studies were discarded from these processes, resulting in 267 articles chosen for further review. To further narrow down the sample size, the researchers implemented an eligibility criteria that included studies with a minimum of 2 citations indexed in Scopus or in SciMago Journal Ranking to ensure data credibility, which resulted in 218 articles. Following this, 120 studies were chosen using a journal assessment matrix and stored in a literature bank located in Google Drive for easy access and convenient storage. The literature's titles, authors, publication years, descriptions, hypotheses, problem statements, objectives, methodologies, results, and discussions were systematically tabulated to summarize key findings. After selection through triangulation, the researchers arrived at a final sample size of 20 articles.

The final sample size was determined by the researchers after a series of meetings discussing the review process, particularly the study selection and data extraction. The three researchers were present to achieve investigator triangulation [67]. In addition to eligibility criteria, the researchers assessed the articles for their empirical credibility through the proposition, testing and evaluation of given solutions. Any discrepancies in the selection process were considered and noted along with justifications for the exclusion of particular studies.

Fig. 2 illustrates the general flow of the researchers' methodology. This review is primarily divided into five main processes: (1) planning the review; (2) selection of primary studies; (3) data extraction, (4) synthesis and results, and; (5) reporting the review.

2.1. Identification, authentication, authorization, and accountability (IAAA) areas of access control in electronic health records

This section describes the qualitative analysis method for synthesizing 20 qualified journals to examine the access control solutions utilized in EHRs. Given the wide array of security solutions (Fig. 3), the researchers have opted to focus the scope on common applications of access control applicable to EHRs identified in the preceding studies [27,65,68,69], namely IAAA. These areas considered are a result of the preceding content analysis and will be the basis for the categorization of the journal articles in this review [27]. The researchers followed the guidelines present in ISO 27002:2022 [70] in classifying and categorizing the articles based on the IAAA access control components. ISO 27002:2022 is a standard designed for any type or size of organization and has been specifically tailored to the implementation and determination of controls for information security risk treatment of existing information systems. This has been implemented to the standard ISO 27799, concerning the information security management needs of the health sector [24,24,55,70–72]. Implementing the guidance from the standard in the context of healthcare organizations is significant (a) to reduce the vulnerability of electronic health records that need protection against various risk sources or incidents, whether natural, accidental, or deliberate; and (b) to enhance confidentiality, integrity, and availability. In addition, this standard provides clear, concise, and specific guidance on the selection and careful classification of methods utilized under Identification, Authentication, Authorization, and Accountability.

For a thorough reading and examination of the final sample size, the researchers utilized hybrid coding for qualitative coding, which is a combination of inductive and deductive coding [73] to gather and extract connected codes, as well as, categorize them into IAAA. Each of the researchers conducted initial coding to have an in-depth understanding and developed an initial set of codes based on the research questions in Table 2. These questions are based on the book utilized from a preceding study [27], entitled, Principle of Information Security [74], and ISO 27002:2022 [70]. Furthermore, by utilizing these questions, the researchers can better comprehend and identify the mechanisms associated with access control, particularly those centered on IAAA. It also provides an opportunity for the researchers to explore the connection between the IAAA mechanisms and how they all contribute to providing information security in EHRs. Afterward, the researchers reviewed the initial codes while re-assessing and combining needed codes. With the pre-established codes, the researchers applied deductive coding in which codes are tallied and categorized into IAAA. To further define the subcategories, the researchers derived brief descriptions and guidelines from the preceding study with its association with Principle of Information Security [74] and ISO 27002:2022 [70], which provide comprehensive coverage of each subcategory.

Identification is a mechanism that focuses on adding a label called an identifier which can either be a composite identifier or a unique identifier, to a supplicant validated by the system. Based on the guidelines from ISO 27002:2022, unique identification and its management according to the assignment to a single person, multiple persons, or non-human entities is prioritized. Since each individual is only connected to one identity, it is easier to hold those identities accountable for the deeds they perform. Shared identities, which are issued to several people, are only permitted when necessary for operational reasons, requiring specific approval and documentation. When identities are no longer required, they are promptly deactivated or removed. Examples of such circumstances include when related entities are deleted or unneeded, when a person departs the company, or when a person changes responsibilities. Thorough documentation is kept of all noteworthy occurrences pertaining to the handling and application of user identities [70].

Authentication is the process where the supplicant is validated based on the provided identifier; it is divided into three mechanisms or factors including what the supplicant knows, something a supplicant has, and that which a supplicant is or can produce. Something a supplicant knows includes a password, passphrase, personal identification number, OTP, and so forth. Something a supplicant has includes ID cards, token cards and ATM cards. Something a supplicant is or can produce include fingerprints, iris scans or hand topography. These factors can be combined into various authentication methods such as single-factor authentication, two-factor authentication, and multi-factor authentication [27,73]. Based on the guidelines from ISO, authentication information must be always kept confidential, especially passwords that are used for authentication. Secure authentication procedures must be used to protect user passwords or personal identification numbers (PINs) that are automatically created during enrollment procedures. These authentication techniques guarantee that each person's produced credentials are distinct and essentially impossible to guess. After their first use, users must update these credentials. Furthermore, strict protocols are implemented to confirm users' identities before granting new, temporary, or replacement login credentials. Information is sent securely and unprotected email messages are not used to preserve the authentication process's integrity. More importantly, careful documentation of important events pertaining to the distribution and maintenance of authentication information is kept, guaranteeing privacy and following accepted

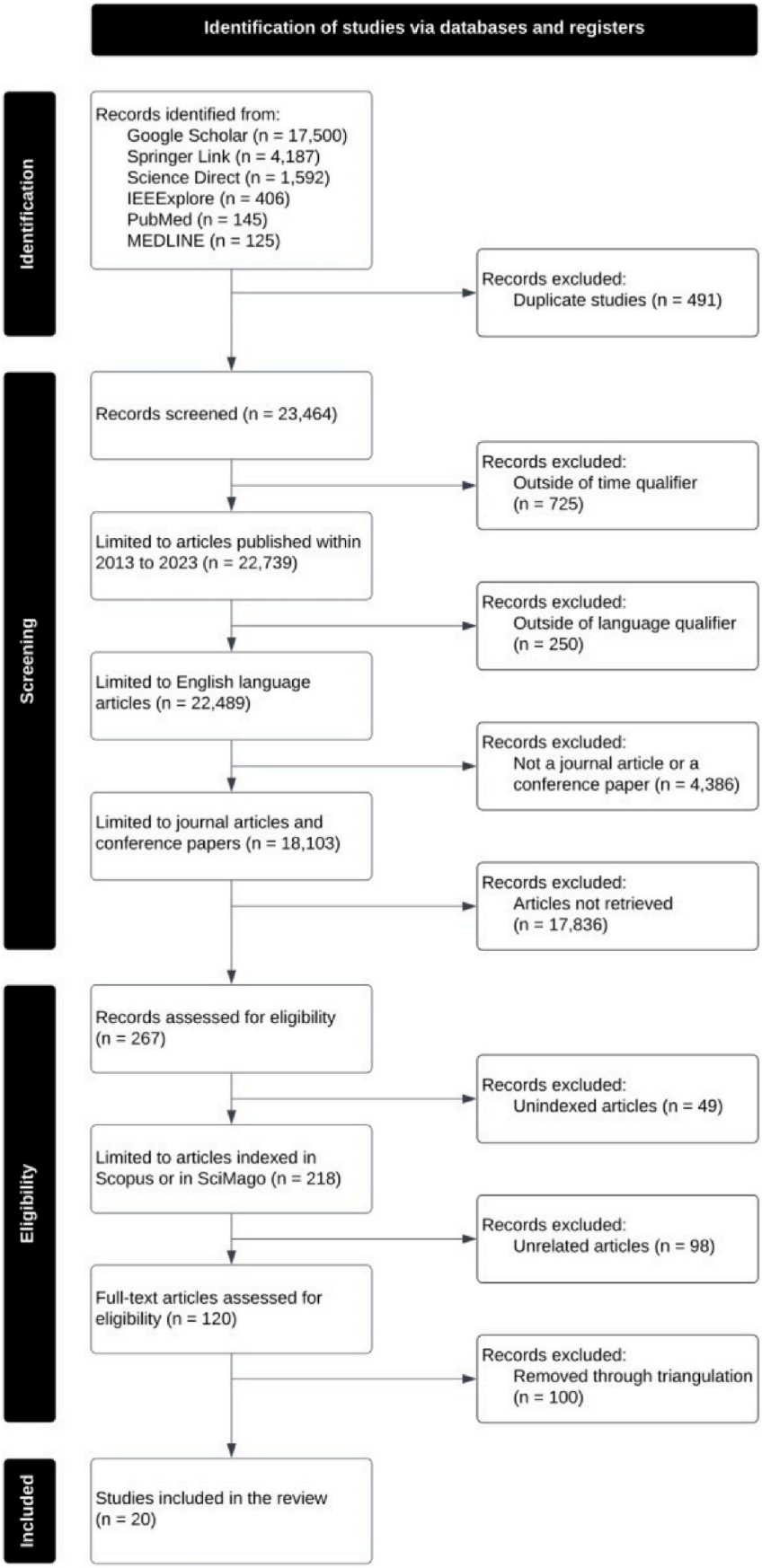

Fig. 1. 2020 PRISMA flowchart.

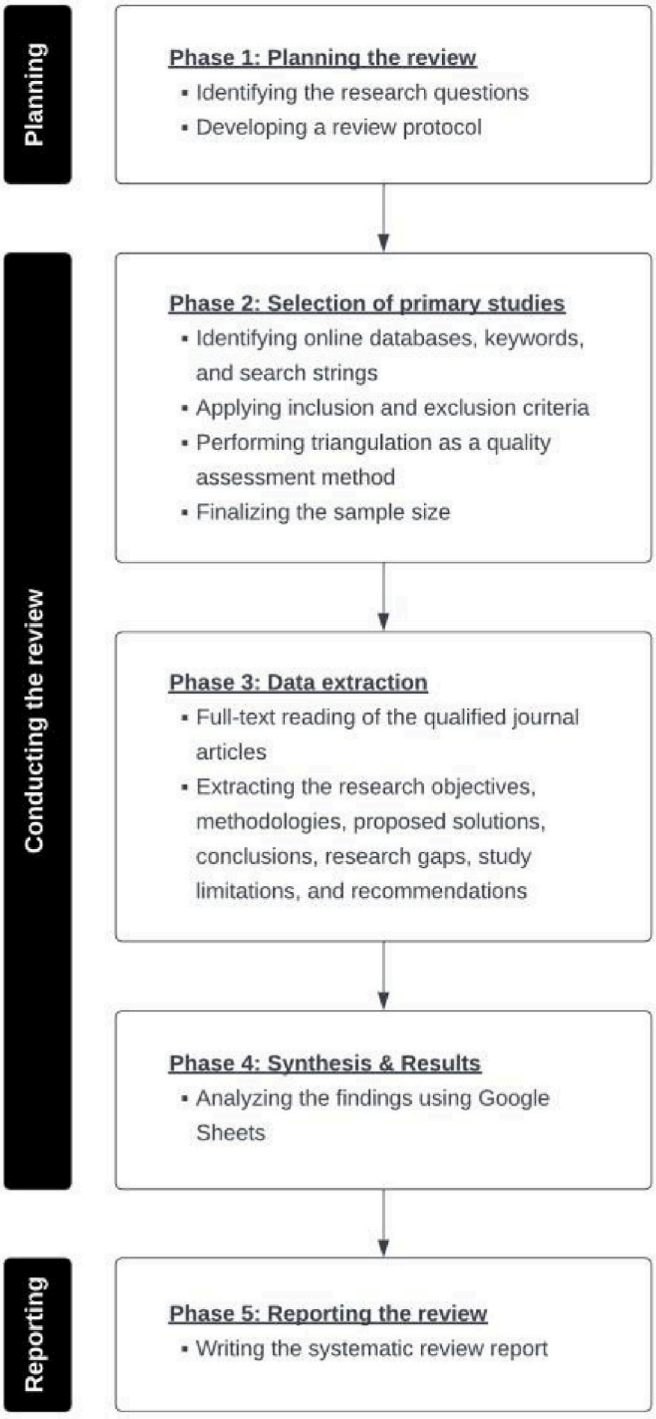

Fig. 2. Methodology flowchart.

record-keeping procedures [70].

Authorization is a component of IAAA that is applicable if the authentication method has succeeded. The focus is to grant authenticated users or entities the necessary permissions based on objects that the users want to access or contexts they are engaged with [70]. Authorization focuses on guaranteeing that authorization and definition of access to data and other related assets follow certain requirements. The identification of authorization schemes was based on the definition and classification of [27,70]. Authorization schemes make use of existing models such as discretionary access control (DAC), attribute-based access control (ABAC), role-based access control (RBAC), and

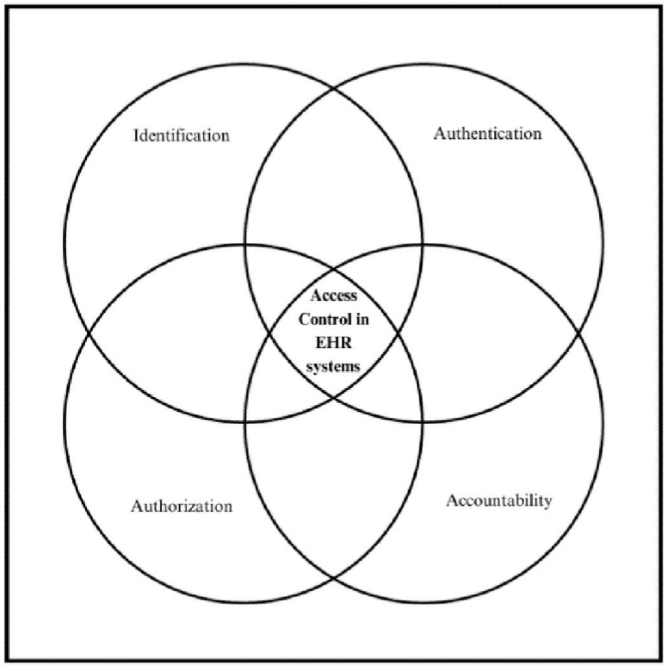

Fig. 3. Access control solutions in electronic health record systems.

Table 2
IAAA-related research questions.

Code	Research questions
Identification	
RQ1	What identifier is applied?
Authentication	
RQ2	What are the authentication mechanisms utilized?
RQ3	What authentication factors are used in the mechanism?
Authorization	
RQ4	What access control models are utilized?
RQ5	Are there access control policies utilized?
RQ6	Is there user authorization?
RQ7	Is there user role identification/assignment?
RQ8	Is there access revocation?
Accountability	
RQ9	Are audit logs utilized?
RQ10	Are there audit mechanisms that are designed and implemented to detect unauthorized use or support incident investigations?
RQ11	Are successful and rejected access attempts recorded?
RQ12	Are transactions made by the users recorded?

mandatory access control (MAC), as well as policies established to grant user-specific requirements before accessing patient data [27,35,36,48,56]. Additionally, the guidelines present in Ref. [70] identify authorization as schemes utilizing access revocation, identifying access rights based on roles, and establishing policies to verify the kind of access a user has.

Audit or accountability is accomplished based on system logs or database journals in which every action of the users is traced and data integrity is maintained. This aims to record incidents, generate evidence, ensure the precision of log data, prevent unauthorized access, and facilitate investigations [46,70,75]. As stated in the ISO 27002:2022, audit logs include keeping track of user-performed transactions within applications, dates, times, and particulars of pertinent events. Additionally, it tracks device identity, system identifier, location, as well as successful and unsuccessful attempts at system access.

2.2. Research gap analysis

This section presents the methodology utilized by the researchers in

conducting a research gap analysis of the 20 articles in the sample literature. A research gap is an unresolved issue in the body of existing research for a particular field of study. It offers insufficient or otherwise missing information that hinders the readers' ability to conclude a specific issue [76]. A research gap analysis for access control solutions in EHRs is conducted to identify these gaps in the body of literature, which will aid future researchers in identifying fruitful areas that require further exploration.

The researchers identified the common conclusions, limitations, and recommendations of the sample literature [77–81] the details of which are discussed in the paragraph that follows. Common conclusions are the recurring, synthesized key points found across several studies of choice [82,83]. These were identified through an examination of the Conclusion & Recommendations sections of the 20 journal articles. On the other hand, common limitations of the study are the prevalent gaps, flaws, and constraints limiting the interpretation of various studies [84–86]. These were discovered through an exhaustive search of the gaps and limitations identified in the systematic reviews on access control solutions for EHRs before supporting excerpts were identified from a full-text examination of the sample literature. Codes that lacked sufficient supporting excerpts were then removed. Furthermore, common recommendations are the consistent suggestions and solutions of numerous studies, which will serve as the direction for future research [79,87]. These were found by analyzing the Results & Discussions and Conclusions & Recommendations sections of the 20 qualified studies in the sample size.

A combination of inductive and deductive qualitative coding was employed in tallying frequently mentioned keywords and in generating initial codes. These codes were then validated and finalized through an assessment of whether they communicated relevant information on access control solutions in EHRs. Finally, similar codes were grouped into themes and a tabulation of the common conclusions, limitations, and recommendations was created to organize existing information and results. A mind mapping technique was then utilized to identify the relationships between the common recommendations for access control solutions in EHRs, as well as to highlight the fruitful areas for further research. Several research gaps were identified after conducting a thematic analysis and synthesis of the articles. The results of the research gap analysis are covered in Section 3.3.

3. Results and discussions

3.1. Identification, authentication, authorization, and accountability (IAAA) areas of access control in electronic health records results

In this section, an examination of prevalent scope and methodologies for access control solutions in EHRs was conducted, focusing on the IAAA aspects within the domain of access control. The 20 qualified journals are synthesized, coded, and synthesized to gain a deeper understanding of the existing breadth and procedures of access control solutions. This is to be able to determine and be familiarized with the common components of the methods under the IAAA category that are utilized for access control solutions in EHRs across different studies to inform future research and discover the meaningful coverage of the application of IAAA. In light of the macro perspective, the researchers have opted to establish the hierarchical structure for the augmented classifications of IAAA from an existing study [27] as the basis of this current study. This will be used to analyze the final sample size and uncover new classifications within the context of access control in EHR. Table 3 presents the summary of the 20 journal articles in the sample size.

Figs. 4 and 5 illustrates the hierarchical structure from an existing study that covers the four areas within the access control in EHR. Before establishing this chart, an analysis is conducted to identify the classification of the methods employed in the areas of identification, authentication, authorization, and accountability. Equally important, the researchers meticulously read and listed the methods associated with each of the four areas in which studies should explicitly indicate those methods which fall within those areas. This analysis seeks to draw the distinction between the methods utilized among the studies from the final sample size and those identified from the previous study. The previous study included biometrics, passwords, public key infrastructure, single sign-on, tokens, smart cards, two-factor authentication, and LDAP as methods under authentication. Additionally, role-based access control, situation-based access control, attribute-based access control, discretionary access control, and mandatory access control as methods under authorization. However, no methods were specified for identification and accountability [27]. In this study the researchers have identified several methods from the final sample size as emphasized below. In addition, given the wide variety of concepts used in access control, the researchers believed that the focus on the areas of identification, authentication, authorization, and accountability helps focus the analysis. It contributes to the decision and selection of the most appropriate solution for the needs of the different healthcare scenarios or contexts in protecting electronic health records.

3.1.1. Identification

The foundation for user authentication is critical for any EHR management, evident in Table 4, wherein the data showed the methods employed for the identification among the twelve studies from the final samp-le size that was applied to this area [35,36,46,48–51,53–57]. In the majority of these studies, unique identification is the most common method. In health institutions utilizing EHRs, user identification is crucial for privacy and confidentiality clauses, securing the health information for the sole use of patient health collaboration among health care providers and at the same time creating efficient workflows allowing on-time accuracy of health care treatment and data mining for accurate health diagnosis and efficient care given. Table 4 shows that the following unique identification is mostly used by the sample size, namely; (1) *User identification* or user ID is an entity used to identify a user on a website, software, system, or within a generic IT environment; (2) *Digital identification,* or electronic identification, refers to the process of validating and establishing the identity of a person or entity via electronic methods; (3) *Identification of the emergency service sessions* that is based on the authentication status and request type as 'Initial Emergency Request' or 'Existing Emergency service Session' received in any EHR and if duly authenticated by the system, then the request will be configured as an Emergency service sessions and access will be granted; and (4) *PKA certification* ensures the safe exchange of symmetric (secret) keys, as well as the computation of digital signatures for message authentication to health care consumers. EHRs have the potential to significantly increase provider-organization collaboration. They can assist everyone in a practice in understanding a patient's requirements, and they allow for simple yet secure information exchange with other physicians or organizations that are critical to the quality of health care delivery. Authenticated and certified identity access in EHRs may enable processes like collecting lab results, issuing referrals, analyzing imaging scans, and e-prescribing medicine easier, faster, and more secure, resulting in better patient care and a simplified clinical workflow.

3.1.2. Authentication

This field is important for authenticating a user's identity and authorizing access before allowing the user access to the data. EHRs, like almost every other computer network today, are subject to hacking, which means sensitive patient data might end up in the wrong hands. While EHRs are supposed to be extremely secure, this danger may still exist, especially if your infrastructure is inadequate. Table 5 shows the methods employed for authentication in which ten of the studies from the final sample size have applied this area [35,36,48,53,55–58,64]. Although these studies [35,36,57,58,64] have not specified the authentication method used, the rest of the researches authentication methods to access control solutions in their EHRs are as follows; (1)

Table 3
Information overview of the 20 qualified journal articles.

Journal ID	Author/s	Title	Year of Publication	Source	Number of Citations	IAAA Category	IAAA Mechanisms
[35]	de Oliveira, M.T., Verginadis, Y., Reis, L.H. A., Psarra, E., Patiniotakis, I., Olabarriaga, S.D.	AC-ABAC: Attribute-based access control for electronic medical records during acute care	2023	Expert Systems with Applications	16	Identification Authentication Authorization	*Identification* • User identification/ authentication identification • Emergency session identification *Authentication* • Mechanism not specified *Authorization* • Access control policies • Attribute-based access control (ABAC) model
[48]	Seol, K., Kim, Y.-G., Lee, E., Seo, Y.-D., & Baik, D.-K.	Privacy-preserving Attribute-based Access Control Model for XML-based Electronic Health Record System	2018	IEEE Access	112	Identification Authentication Authorization	*Identification* • Unique identification *Authentication* • Digital signature *Authorization* • Access control policies • Attribute-based access control (ABAC) model
[36]	Rivera Sánchez, Demurjian, S. A., & Baihan, M. S.	A service-based RBAC & MAC approach incorporated into the FHIR standard	2019	Digital Communications and Networks	16	Identification Authentication Authorization	*Identification* • Unique identification *Authentication* • Mechanism not specified *Authorization* • Mandatory access control model (MAC) • Role-based access control model (RBAC)
[33]	Bhartiya, S., Mehrotra, D., & Girdhar, A.	Proposing hierarchy-similarity based access control framework: A multilevel Electronic Health Record data sharing approach for interoperable environment	2017	Journal of King Saud University - Computer and Information Sciences	25	Authorization	Access control policies User authorization
[37]	Abomhara, M., Yang, H., Køien, G. M., & Lazreg, M. B.	Work-Based Access Control Model for Cooperative Healthcare Environments: Formal Specification and Verification	2017	Journal of Healthcare Informatics Research	10	Authorization	Work-based access control model (WBAC) Access control policies Access revocation User role Assignment
[60]	Guesmia, K., & Boustia, N.	OrBAC from access control model to access usage model	2017	Applied Intelligence	8	Authorization	*P*- Organization based access control (*P*-OrBAC) model
[56]	Gardiyawasam Pussewalage, H. S., & Oleshchuk, V. A.	Attribute based access control scheme with controlled access delegation for collaborative E-health environments	2017	Journal of Information Security and Applications	33	Identification Authentication Authorization	*Identification* • PKI certificate *Authentication* • Digital signature • Mutual authentication • PKI Authentication *Authorization*

(*continued on next page*)

Table 3 (*continued*)

Journal ID	Author/s	Title	Year of Publication	Source	Number of Citations	IAAA Category	IAAA Mechanisms
							• Attribute-based access control (ABAC) model • Access revocation
[57]	Mhatre, S., & Nimkar, A. V.	Secure Cloud-Based Federation for EHR Using Multi-authority ABE	2018	Progress in Advanced Computing and Intelligent Engineering	16	Identification Authentication Authorization	*Identification* • Unique identification • User identification/ authentication identification *Authentication* • Mechanism not specified *Authorization* • Access revocation • Ciphertext-policy attribute-based encryption (CP-ABE) scheme
[49]	Guo, C., Zhuang, R., Jie, Y., Ren, Y., Wu, T., & Choo, K.-K. R.	Fine-grained Database Field Search Using Attribute-Based Encryption for *E*-Healthcare Clouds	2016	Journal of Medical Systems	113	Identification Authorization	*Identification* • Unique identification *Authorization* • Ciphertext-policy attribute-based encryption (CP-ABE) scheme
[50]	Zhang, A., Bacchus, A., & Lin, X.	Consent-based access control for secure and privacy-preserving health information exchange	2016	Security and Communication Networks	29	Identification Authentication Authorization	*Identification* • Unique identification • User identification/ authentication identification *Authentication* • Mutual authentication • Signature algorithm *Authorization* • Consent-based access control protocol (CBAC) • Access revocation
[51]	Sicuranza, M., Esposito, A., & Ciampi, M.	An access control model to minimize the data exchange in the information retrieval	2015	Journal of Ambient Intelligence and Humanized Computing	22	Identification Authorization	*Identification* • User identification/ authentication identification *Authorization* • Temporal model-based access control • Access control policies • User role Assignment • Role-based access control model (RBAC)
[64]	Soceanu, A., Vasylenko, M., Egner, A., & Muntean, T.	Managing the privacy and security of ehealth data	2015	2015 20th International Conference on Control Systems and Computer Science	42	Authentication Authorization	*Authentication* • Mechanism not specified *Authorization* • Access control policies

(*continued on next page*)

Table 3 (*continued*)

Journal ID	Author/s	Title	Year of Publication	Source	Number of Citations	IAAA Category	IAAA Mechanisms
							• Attribute-based access control (ABAC) model
[52]	Zhang, X., Poslad, S., & Ma, Z.	Block-based access control for blockchain-based electronic medical records (EMRs) query in eHealth	2018	2018 IEEE Global Communications Conference (GLOBECOM)	43	Authorization	Block-based access control scheme (BCAC) User authorization
[53]	Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y.	A smart-contract-based access control framework for cloud smart healthcare system	2020	IEEE Internet of Things Journal	136	Identification Authentication Authorization	*Identification* • Unique identification *Authentication* • Digital signature *Authorization* • Smart contract based access control framework • Access revocation
[54]	M. B. Smithamol, S. Rajeswari	Hybrid Solution for Privacy-Preserving Access Control for Healthcare Data	2017	Advances in Electrical and Computer Engineering	20	Identification Authorization	*Identification* • Unique identification *Authorization* • Access control policies • Ciphertext-policy attribute-based encryption (CP-ABE) scheme
[58]	Chinnasamy, P., & Deepalakshmi, P.	HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud	2021	Journal of Ambient Intelligence and Humanized Computing	66	Authentication Authorization	*Authentication* • Double authentication *Authorization* • User authorization
[46]	Guo, H., Li, W., Nejad, M., & Shen, C.-C.	Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture	2019	2019 IEEE International Conference on Blockchain (Blockchain)	168	Identification Authorization Accountability	*Identification* • Unique identification • User identification/ authentication identification • Digital identification *Authorization* • Access control policies *Accountability* • Access control logs
[75]	Jaiman, V., & Urovi, V.	A Consent Model for Blockchain-Based Health Data Sharing Platforms	2020	IEEE Access	99	Authorization Accountability	*Authorization* • Blockchain-based data sharing consent model • Access control policies *Accountability* • Transaction history
[59]	Psarra, E.; Apostolou, D.; Verginadis, Y.; Patiniotakis, I.; Mentzas, G.	Context-Based, Predictive Access Control to Electronic Health Records	2022	Electronics	7	Authorization	Attribute-based access control (ABAC) model
[55]	Zhao, F., Yu, J., & Yan, B.	Towards cross-chain access control model for medical data sharing	2022	Procedia Computer Science	13	Identification Authentication Authorization	*Identification* • Unique identification • Digital identification

(*continued on next page*)

Table 3 (*continued*)

Journal ID	Author/s	Title	Year of Publication	Source	Number of Citations	IAAA Category	IAAA Mechanisms
							Authentication • Digital signature *Authorization* • Cross-chain based access control model

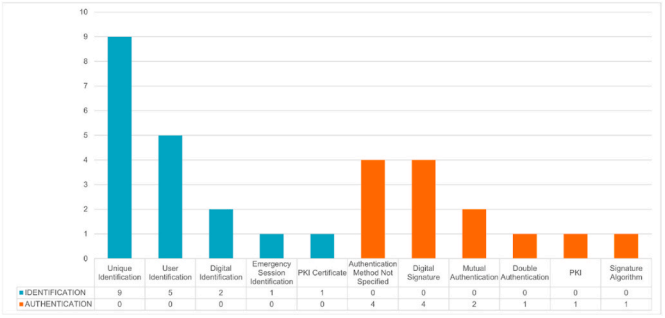

Fig. 4. Identification and authentication components of access control solutions in EHRs.

Digital signature, wherein an electronic, encrypted authenticating stamp on digital information such as emails, macros, or electronic documents; (2) *Mutual authentication, is when both sides of a communication channel check each other's identity*, rather than merely one side validating the other; (3) *Double authentication*, often known as two-factor authentication (2FA), is a security mechanism that needs two independent forms of identity in order to get access to anything. The first factor is a password, and the second is often an SMS with a code delivered to your smartphone, or biometrics such as your fingerprint, face, or retina; and (4) *Public Key Infrastructure (PKI)*, a widely established protocol for standardizing digital signatures that give the greatest levels of security and universal acceptance, this includes the use of a digital certificate to verify identities, and signature algorithm. This signature algorithm is the public-key equivalent of a message authentication code. It is composed of three parts; (1) a key generation algorithm that can be shared with other public-key algorithms; (2) a signature generation algorithm and (3) a signature verification algorithm. Signature algorithms may be created utilizing encryption methods. Using the private key, we generate a value based on the message, often using a cryptographic hash. Anyone may then use the public key to obtain that value, compute what it should be based on the message, and compare the two to validate. The apparent distinction between this and public-key encryption is that in signing, the private key is used to create the message (in this example, the signature), while the public key is used to understand it, which is the inverse of how encryption and decryption function. Because of the instantaneous nature of electronic health records, they must be updated and authenticated

Table 4
Identification methods of access control solutions in EHR systems.

Methods	Count	References
Unique identification	9	[36,46,48–50,53–55,57]
User identification/authentication identification	5	[35,46,50,51,57]
Digital identification	2	[46,55]
Emergency session identification	1	[35]
PKI certificate	1	[56]

Table 5
Authentication methods of access control solutions in EHR systems.

Methods	Count	References
Authentication method not specified	5	[35,36,57,64]
Digital signature	4	[48,53,55,56]
Mutual authentication	2	[50,56]
Double authentication	1	[58]
PKI	1	[56]
Signature algorithm	1	[50]

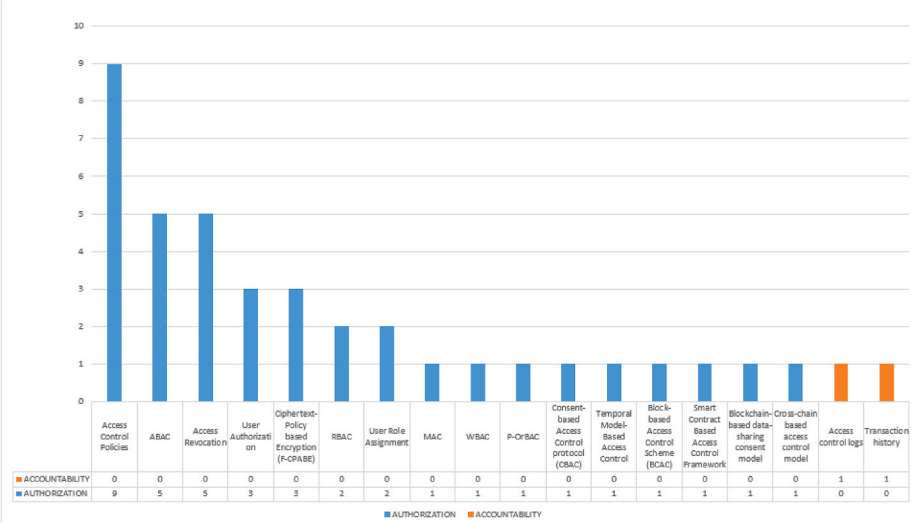

Fig. 5. Authorization and accountability components of access control solutions in EHRs.

immediately after every health personnel and system changes that could access the health information. Failure to do so could be detrimental to the privacy and security measures, as well as quality healthcare treatment since healthcare providers will rely on the current 'perceived' authenticated data when determining appropriate treatment protocols.

3.1.3. Authorization

This section is important because it allows the subject to access a certain resource and conduct actions on that resource based on the permissions given. Access control systems manage and limit access to resources, systems, and physical regions inside health institutions and organizations or health data systems.

Controlled information and resources may only be accessed by authorized health practitioners with the right authority; for example, access to laboratory information from a medical technologist or radiology department may be restricted to them and patients, doctors or healthcare team for management, and these electronic medical data should be accessible only to authorized personnel.

Table 6 shows the methods employed for authorization in which the 20 studies from the final sample size have applied this area [33,35–37,48,56,60]. According to the findings of the study, access control policies are the most prevalent way for securing sensitive data and lowering the danger of an attack. Access control policies work by validating user credentials, establishing their identity, and granting pre-approved access based on their username and IP address. This is followed by; (1) *Attribute-based access control (ABAC)*, also referred to as policy-based access control (PBAC) or claims-based access control (CBAC), is an authorization methodology that sets and enforces policies based on characteristics, such as department, location, manager, and time of day; (2) *Access Revocation,* which revoke the entire account from a health care personnel and other healthcare management staff. This is frequently used when a healthcare member departs a firm or when a user violates the terms of service for a particular service. When an account is revoked, all access to the resources connected with it is removed; (3) *Ciphertext-Policy Attribute-Based Encryption (CP-ABE)* Scheme is where data is encrypted by the data owner using an attribute-based access structure before being sent to the storage service, and only users with permitted sets of attributes may successfully decode the produced ciphertext. The ciphertext-policy attribute-based encryption (*C*P-ABE) technique includes three articles: user authorization, user role assignment, and the role-based access control (RBAC) model. Both user authorization and user role assignment are the granting of certain health care personnel/user certain rights to access information by assigning at least one individual for the specific responsibility. This personnel/user can access the EHR data and resources that have been assigned and subsequently authorized to retrieve and access the health information.

Table 6
Authorization methods of access control solutions in EHR systems.

Methods	Count	References
Access control policies	9	[33,35,37,46,48,51,54,64,75]
Attribute-based access control (ABAC) model	5	[35,48,56,59,64]
Access revocation	5	[37,50,53,56,57]
Ciphertext-policy attribute-based encryption (*C*P-ABE) scheme	3	[49,54,57]
User authorization	3	[33,52,58]
User role Assignment	2	[37,51]
Role-based access control model (RBAC)	2	[36,51]
Mandatory access control model (MAC)	1	[36]
P- Organization based access control (*P*-OrBAC) model	1	[60]
Work-based access control model (WBAC)	1	[37]
Consent-based access control protocol (CBAC)	1	[50]
Temporal model-based access control	1	[51]
Block-based access control scheme (BCAC)	1	[52]
Smart contract based access control framework	1	[53]
Blockchain-based data sharing consent model	1	[75]
Cross-chain based access control model	1	[55]

3.1.4. Accountability

This section is critical because it gives users complete control over when and how they access certain EHRs. Table 7 shows that only two of the studies from the final sample size utilized audit mechanisms via accountability methods of access control solutions in EHRs [46,75].

When analyzing the literature, the researchers found that there is a connection of each of the components in security systems. These components are IAAA access control mechanisms. Among the study reviews, the commonly used combinations were authentication and authorization with a total of five studies [36,48,50,57,58]. Privacy and security are of prime importance to the healthcare management to secure vital health information from patients and their medical cases. EHRs must comply with the Health Insurance Portability and Accountability Act (HIPAA), which requires comprehensive mechanisms for access control, information preservation, and audit recording. Authentication and permission are necessary security measures for a health facility. The authentication process identifies a user; the user is granted permission (authority) to execute a specific task; and the accounting process tracks how the health information data was used and who utilized it. There are two studies for each of those that have used the four components of IAAA and a combination of identification, authorization, and authentication [46,53,55,56]. There was only one study that used each of the following combinations: authentication, authorization, and accountability [64]; authorization and accountability [75]; and identification and authorization [35]. There are various possible liability risks related to EHR installation. A patient's medical data might be lost or deleted during the shift from a paper-based to a digital EHRs, potentially leading to treatment mistakes and malpractice liability concerns. Because EHR provides doctors with more access to medical data, they may be held accountable if they do not use all of the information available to them and at the same time the health care management/institution can also be liable over privacy and security risks which result in data accuracy issues.

3.2. Research gap analysis results

3.2.1. Common conclusions

This section discusses the common conclusions in the sample literature of access control solutions in EHRs. As shown in Table 8, the majority of the studies are partially adherent to information security requirements [33,35,37,48–53,55,56,58–60,64,75]. Partial adherence is a term used to describe access control solutions that fail to fully adhere to information security standards and requirements; typically, at least one requirement is overlooked or ignored [34,88]. Be that as it may, at least one security requirement is still met by the proposed access control solutions, which serves as the baseline for developing fine-grained access control [33,35–37,46,48–51,54,56,57,60,64,75]. Additionally, interoperability is another feature of access control in EHRs [33,36,37,48,50,55–58,75]. It is a crucial component in securing patient health information exchange between healthcare entities. It shows that legitimate, authorized access is necessary for ensuring data confidentiality [33,35,46,49,51,53,55,56,64]. Moreover, the proposed access control solutions demonstrate feasibility in real-world EHRs and healthcare environments [33,35,37,46,48,53,54,56]. These common conclusions emphasize the importance of implementing well-designed, fine-grained access control solutions for securing patient health information in EHRs.

Table 7
Accountability methods of access control solutions in EHR systems.

Methods	Count	References
Access control logs	1	[46]
Transaction history	1	[75]

Table 8
Common conclusions of access control solutions in EHR systems.

Common Conclusions	Count	References
Partial adherence to information security requirements	16	[33,35,37,48–53,55,56,58–60,64,75]
Provides flexible, fine-grained access control	15	[33,35–37,46,48–51,54,56,57,60,64,75]
Achieves interoperability	10	[33,36,37,48,50,55–58,75]
Provides legitimate, authorized access	9	[33,35,46,49,51,53,55,56,64]
Feasible for real-world implementation	8	[33,35,37,46,48,53,54,56]

3.2.2. Common gaps & limitations

This section discusses the identified gaps and limitations in the sample literature of access control solutions in EHRs. A total of nine limitations were identified from the sample literature and categorized into four main categories, namely: (1) *Methodology implementation limitations;* (2) *Standards & regulations compliance limitations;* (3) *Implementation and evaluation limitations,* and; (4) *Data availability limitations.*

As shown in Table 9, the most mentioned literature gaps in the sample size are the methodology implementation limitation and the information security compliance limitation. The former reveals the non-implementation of specific mechanisms in access control solutions for EHRs, such as lack of two-factor or multi-factor authentication [33,35–37,46,48–57,59,60,64,75], lack of accountability [33,35–37,48–60,64], lack of patient consent [33,36,37,49,52,56–58], and few discussions about emergency access [33,36,37,46,49,50,52,53,55–58,64,75]. Either it has been demonstrated that these mechanisms are more reliable than previous methods, or that several information security standards require them as security measures. Their absence leaves EHRs open to unauthorized access. On the other hand, the information security compliance limitation category includes non-compliance to information security standards [33,36,37,46,49,52–56,58–60] and a lack of a harmonized policy/standard for information security [35,48,50,51,57,64,75]. Non-compliance carries a number of risks, the most important of which is that the studies' validity may be called into question. Furthermore, the lack of a harmonized standard leads to policy and guideline inconsistencies. These conflicting views may cause healthcare organizations to select a security framework which may fit their needs, but may not offer complete privacy of patient information. Another factor is the implementation and evaluation limitation, that is, the lack of implementation in a real-world environment [33,35,37,46,48–60,64,75]. Data availability limitations have been identified from the sample literature, which includes the unavailability of source code and testing dataset copies for systematic benchmarking [36,37,46,48–54,56–60,64,75]. These limitations reveal important areas for research and allow the researchers to contextualize the findings in this study.

3.2.3. Common recommendations

This section discusses the common recommendations for future research endeavors according to the 20 articles analyzed. A total of fourteen recommendations were identified from the sample literature and categorized into four main categories, namely: (1) *Further refinement of the methodology;* (2) *Widening the testing scope;* (3) *Generalization of the proposed solutions,* and; (4) *Implementation of additional laws and regulations for specific contexts.*

Table 9
Common limitations of access control solutions in EHR systems.

Common Limitations	Count	References
Methodology implementation limitation	20	[33,35–37,46,48–60,64,75]
Standards & regulations compliance limitation	20	[33,35–37,46,48–60,64,75]
Implementation and evaluation limitation	19	[33,35,37,46,48–60,64,75]
Data availability limitation	17	[36,37,46,48–54,56–60,64,75]

As shown in Table 10 and Fig. 6, there is a need for further refinement of the proposed methodologies. Extending the proposed solution with additional access control models [33,35,36,46,48–50,52,53,55–57,60], refining the access control policies [33,60], validating and widening the scope [54,58,59], and integrating technological systems into the methodology [51,64] have been recommended in the sample literature. Other recommendations involve broadening the testing scope, which involves evaluating the performance and scalability of the proposed methodology [37,48,49,51,52,60,75], and developing tools for effective evaluation [46]. Further the literature recommends investigating cross-border healthcare collaboration, expanding the prototype implementation [37,48], and expanding the testing phase by conducting an additional evaluation of proposed solutions against other models [36], while simulating larger tests [75], and conducting field tests [37,49,51,54,57]. It is necessary to investigate the generalization of the proposed methodology in order to derive solutions that are applicable in differing contexts [36]. Lastly, there is a need to implement additional laws and regulations that specify the tasks that must beperformed in particular contexts, such as those involving emergencies or contingencies [60].

3.3. Discussions

3.3.1. Key findings on authentication-related access control solutions in EHRs

The majority of the articles in the sample size utilize digital signatures for authentication, which uses a private key to encrypt the signature data before it is decrypted by a public key. It enables end-to-end encryption of messages and various resources, ensuring secure communication and message integrity. The results of the study show similarity with those of [24], which states that digital signatures are frequently used data authentication methods for EHRs. As for user authentication, this study found that mutual authentication was most used, while usernames/passwords were also common [24]. Another study, however, reveals that biometric authentication is highly tagged in their sample literature [27]. While the frequency of the tags does not indicate its efficacy, it does imply that biometrics is most frequently used. These authentication methods fall under the category of single-factor authentication (SFA) methods, which has been shown to be less secure than two-factor (2FA) or multi-factor authentication (MFA). SFAs are vulnerable to cybersecurity attacks since they only require one credential to gain access to the EHR. Interestingly, the researchers found that there is a lack of 2FA or MFA in the sample studies. Unlike SFA, MFA requires two or more credentials for verifying user identity. Even if one of the required credentials has been compromised, without the other one, users are still unable to gain access to the EHR and its sensitive information. For these reasons, several studies recommend the use of 2FA or MFA [24,27,89–93].

3.3.2. Key findings on authorization-related access control solutions in EHRs

A salient aspect in the results of our study and [24] was observed in terms of authorization models and policies. Among the different categories of access control approaches, authorization was the most utilized mechanism. According to the results of our investigation, the most

Table 10
Common recommendations of access control solutions in EHR systems.

Common Recommendations	Count	References
Further refine the methodology	18	[33,35,36,46,48–60,64]
Widen the testing scope	11	[36,37,46,48,49,51,52,54,57,60,75]
Explore the generalization of the proposed solutions	1	[36]
Implement additional laws & regulations for specific contexts	1	[60]

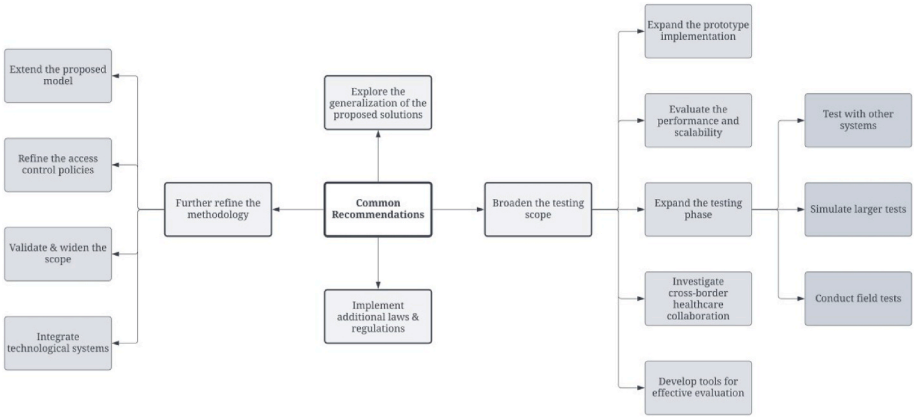

Fig. 6. Common recommendations of access control solutions in EHRs.

widely utilized type is attribute-based access control (ABAC). However [24], states that role-based access control (RBAC) is proposed by the majority of their studies. Another study reveals that studies proposing RBAC usually extend the model with additional components for flexibility [25]. Despite this [24], it suggests ABAC as a better alternative as ABAC offers greater flexibility over traditional access control models by granting access based on attributes or characteristics. It is capable of defining specific policies for specific contexts by combining subject, resource, environment, and action attributes for fine-grained access control. Emergency access is another security feature present in EHRs. It pertains to a set of documented procedures as a requirement for healthcare entities to bypass certain security measures that prevent others from accessing patient information under normal circumstances. The lack of emergency access is a prominent gap in the sample literature as an essential mechanism for healthcare providers and organizations to gain access to a patient's EHR in emergency cases when consent cannot be obtained. Without these mechanisms in place, critical treatment may be delayed due to the unavailability of the patients' EHRs [24,94] so studies often recommend its implementation [24,27,43,94,95].

Furthermore, consent is a component of another authorization model involving the patients themselves. Patient consent refers to the process where patients grant permissions to healthcare providers to access their EHRs. Under the HIPAA Privacy Rule, patient consent is covered, but not required [96–98]. Healthcare entities may still gain access to patients' EHRs without their consent and in certain situations, may even share patients' protected health information (PHI) with other healthcare providers. On the other hand, the GDPR information security standard maintains that patient consent must always be obtained, particularly during patient care. Patients should have the autonomy to control the security and privacy of their EHRs, and one way of doing that is by limiting who has access to their medical records. The lack of patient consent, however, is an additional limitation in the literature. The lack of patient consent may lead to medical malpractice since it is an ethical and legal requirement for medical treatment. Since EHRs contain a patient's medical history, the researchers could argue that EHRs are a part of medical treatment procedures. Thus, informed consent is fundamental in the healthcare setting. Several articles believe that obtaining patient consent before accessing medical records is a requirement of patient care [24,25,94,99]. One study also believes on the contrary, that exceptions to patient consent should be made for particular circumstances [88]. Another study suggests that patient controls should follow the guidelines and standards according to specific, local requirements [66]. The researchers, however, believe that patient consent is a standard necessity for proper patient care.

3.3.3. Key findings on accountability-related access control solutions in EHRs

As aforementioned, access control comprises four main categories, one of which includes accountability or auditing. By satisfying the accountability requirement, access to medical data is monitored in terms of who accessed the EHR, what action was performed, and when was the action performed [24]. One study states that auditing requires frequent monitoring of every activity occurring in a healthcare system [88]. Two other studies point out the importance of auditing during emergency access, to make users responsible for their actions during this period [27]. Two articles argue that auditing could also be used to study clinical activity for structuring informatics tools and for improving clinical decision-making efforts [100,101]. There is a significant difference in the results presented in terms of accountability or auditing mechanisms. In their results, it is evidenced that many EHRs rely on the auditing of log data. On the other hand, the research gap analysis conducted in this study presents the lack of accountability or audit mechanisms in general. Without these mechanisms, authorized and unauthorized users can escape detection for their potential misuse of patient information [24]. There is no guarantee of security & privacy of health data since there is a lack of records that track user actions in EHRs.

3.3.4. Additional discussions

From the results, it is evident that different IAAA methods intersect, that is, access control solutions utilize one or a combination of IAAA components to ensure patient information confidentiality in EHRs. In this way, access control is dependent on the components of IAAA [27].

On another note, although our study provided a thorough analysis of the sample size, it is essential to consider other topic dimensions to ensure an effective and secure application of these methodologies. The first aspect to consider is access control solutions for healthcare data sharing. Four studies [35,50,55,75] in our sample size have proposed secure access control methods for exchanging healthcare data, taking into account different lenses for (a) smooth cross-organization data sharing encompassing different teams during acute care [35]; (b) cloud-based data sharing scheme requiring the condition of consent from the data owner and providing temporary access to their data [50]; (c) individuals that set and modify data use conditions and various access based on consent in different scenarios [55], and; (d) specific access rights between patient and doctors ensuring secure, patient-centric data sharing [75]. Despite the presence of these studies, this review doesn't fully address the need for a comprehensive examination of the extent of secure access control mechanisms in healthcare data sharing. Another review can concentrate solely on the increased vulnerabilities in the breadth of healthcare data sharing encompassing numerous entities or healthcare providers, and examine advanced secure access mechanisms providing effective access rights or preventing unauthorized access in this context. For instance Ref. [102], proposed an innovative retrieval method which provides secure access to healthcare-shared data stored in cloud repositories by allowing the cloud location of the healthcare data stored in the indexing database. In emergencies where patients are

unable to provide consent, this method enables healthcare providers to retrieve and return the necessary patient data without the need for direct access credentials to the patients' cloud repository. Another aspect to examine that wasn't covered in this study is environmental sustainability. This subject has been extensively studied in other research areas; one such study found that numerous higher education institutions had incorporated environmental sustainability policies and identified challenges to adopting green ICT practices [103]. On the other hand, another study focused on the energy efficiency of their proposed solution in cloud computing, which minimizes carbon emissions [104]. The researchers believe that environmental sustainability must be incorporated into the healthcare setting if the industry seeks to align its practices with the sustainable development goals (SDGs). Hence, another study can be conducted solely to determine the energy efficiency of proposed access control mechanisms in EHRs. This is to determine which solution is more sustainable and suitable for use while adhering to the available environmental sustainability metrics.

4. Conclusion & Recommendations

This study provides a systematic review analysis on the existing literature of access control solutions in EHRs. As a security mechanism, access control enables data owners to grant users access and restrict which users are permitted to read, execute, distribute, and alter system resources. This paper synthesized 20 journal articles to investigate what has been done in the literature regarding access control. The study focused on four components namely Identification, Authentication, Authorization, and Auditing (IAAA). The researchers analyzed the sample size articles, categorized each variable and applied qualitative analysis with the use of ISO 27002:2022. A combination of inductive and deductive coding was used to determine the variables of each study. Findings reveal that the majority of the proposed scheme uses authorization, where ABAC is considered the most flexible authorization model for creating fine-grained access control. Additionally, digital signatures are commonly used as an authentication mechanism. Access control solutions in EHRs don't fully comply with information security standards, and some proposed solutions only partially comply with privacy requirements. The results presented in this study reveal directions and salient areas for future research. We suggest further exploration in the implementation of multi-factor authentication, accountability mechanisms, emergency access, and patient consent. Additionally, further investigation must also be conducted on access control solutions for healthcare data sharing and environmental sustainability, particularly on the energy efficiency of certain access control mechanisms in EHRs. Despite not being originally tackled in the IAAA framework, the research process discovered additional gaps and limitations from the sample literature that may warrant further investigation in future works.

A limitation of the study was that the framework used was largely limited to IAAA access control mechanisms and IAAA-related security controls identified from the ISO 27002:2022 standard. In relation to this, the search string is biased towards the IAAA key terms. It also contains the researchers' bias for particular access control mechanisms conceived at the outset of the study. In addition, the researchers would like to highlight the exclusion of studies that were written by authors or sources that didn't offer free reading of their work. The researchers deemed that the qualified articles to be examined should be available to the public or have open access for increased visibility for readers. The researchers felt that without subscription barriers and the presence of open-access research, the study would have a wider audience and could assist curious minds worldwide. However, it couldn't be denied that this is one limitation of the study as other scholastic journals that contribute to the topic might have been missed. Further, the review only included English articles published between 2013 and 2023. During the triangulation method, it is possible that the researchers may have discarded pertinent studies on access control solutions in EHRs to obtain 20 articles for the final sample size that some may find insufficient. The research lens of the study was centered on security and privacy concerns within the context of healthcare, which may not necessarily capture other relevant access control-related and EHR-related issues in other industries. The researchers centered the scope of the study to IAAA access control mechanisms and selected databases which similar systematic reviews have used. Thus, some articles which supposedly satisfied the researchers' criteria for the study might've been overlooked. Future research can amend these limitations by venturing outside of the scope of IAAA access control mechanisms in the healthcare context, as well as increasing the sample to a more comprehensive size.

Funding

The study is a systematic review, hence no funding was required.

Ethical Statement for informatic medicine unlocked

1) This material is the authors' own original work, which has not been previously published elsewhere.
2) The paper is not currently being considered for publication elsewhere.
3) The paper reflects the authors' own research and analysis in a truthful and complete manner.
4) The paper properly credits the meaningful contributions of co-authors and co-researchers.
5) The results are appropriately placed in the context of prior and existing research.
6) All sources used are properly disclosed (correct citation). Literally copying of text must be indicated as such by using quotation marks and giving proper reference.
7) All authors have been personally and actively involved in substantial work leading to the paper, and will take public responsibility for its content.

The violation of the Ethical Statement rules may result in severe consequences.

To verify originality, your article may be checked by the originality detection software iThenticate. See also http://www.elsevier.com/editors/plagdetect.

CRediT authorship contribution statement

Usha Nicole Cobrado: Writing – original draft. **Suad Sharief:** Writing – original draft. **Noven Grace Regahal:** Writing – original draft. **Erik Zepka:** Writing – original draft. **Minnie Mamauag:** Writing – original draft. **Lemuel Clark Velasco:** Writing – original draft.

Declaration of competing interest

All listed authors declare no competing interests.

Acknowledgements

The authors would like to acknowledge the Mindanao State University-Iligan Institute of Technology (MSU-IIT), specifically the Department of Research from the Office of the Vice Chancellor for Research and Enterprise and the WE CARE Office from the Office of the Vice Chancellor for Public Affairs for their assistance in this study. The authors would also like to thank ILIGANiCE (Innovation thru Leveraging Industry, Government, Academe Networks and inclusive Community Engagements) for their assistance in this study.

References

[1] Yuan B, Li J. The policy effect of the general data protection regulation (GDPR) on the digital public health sector in the European union: an empirical

investigation. Int J Environ Res Publ Health Mar. 2019;16(6):1070. https://doi.org/10.3390/ijerph16061070.
[2] Seh AH, et al. Healthcare data breaches: insights and implications. Healthc. Basel Switz. May 2020;8(2):133. https://doi.org/10.3390/healthcare8020133.
[3] Nifakos S, et al. Influence of human factors on cyber security within healthcare organisations: a systematic review. Sensors Jul. 2021;21(15):5119. https://doi.org/10.3390/s21155119.
[4] Pool J, Akhlaghpour S, Fatehi F, Burton-Jones A. A systematic analysis of failures in protecting personal health data: a scoping review. Int J Inf Manag Feb. 2024;74:102719. https://doi.org/10.1016/j.ijinfomgt.2023.102719.
[5] K. Haan and K. Main, "EHR vs EMR: What's The Difference?," Forbes Advisor. Accessed: October. 25, 2023. [Online]. Available: https://www.forbes.com/advisor/business/software/ehr-vs-emr/.
[6] Yang J-J, Li J-Q, Niu Y. A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Generat Comput Syst Feb. 2015;43(44):74–86. https://doi.org/10.1016/j.future.2014.06.004.
[7] Shen N, et al. Understanding the patient privacy perspective on health information exchange: a systematic review. Int J Med Inf May 2019;125:1–12. https://doi.org/10.1016/j.ijmedinf.2019.01.014.
[8] Entzeridou E, Markopoulou E, Mollaki V. Public and physician's expectations and ethical concerns about electronic health record: benefits outweigh risks except for information security. Int J Med Inf Feb. 2018;110:98–107. https://doi.org/10.1016/j.ijmedinf.2017.12.004.
[9] Mbonihankuye S, Nkunzimana A, Ndagijimana A. "Healthcare data security technology: HIPAA compliance," wirel. Commun Mob Comput Oct. 2019;2019:1–7. https://doi.org/10.1155/2019/1927495.
[10] Oh S-R, Seo Y-D, Lee E, Kim Y-G. A comprehensive survey on security and privacy for electronic health data. Int J Environ Res Publ Health Sep. 2021;18(18):9668. https://doi.org/10.3390/ijerph18189668.
[11] Enaizan O, Eneizan B, Almaaitah M, Al-Radaideh AT, Saleh AM. Effects of privacy and security on the acceptance and usage of EMR: the mediating role of trust on the basis of multiple perspectives. Inform Med Unlocked 2020;21:100450. https://doi.org/10.1016/j.imu.2020.100450.
[12] Vimalachandran P, Liu H, Lin Y, Ji K, Wang H, Zhang Y. Improving accessibility of the Australian My Health Records while preserving privacy and security of the system. Health Inf Sci Syst Dec. 2020;8(1):31. https://doi.org/10.1007/s13755-020-00126-4.
[13] Bani Issa W, et al. Privacy, confidentiality, security and patient safety concerns about electronic health records. Int Nurs Rev Jun. 2020;67(2):218–30. https://doi.org/10.1111/inr.12585.
[14] Kim KK, Joseph JG, Ohno-Machado L. Comparison of consumers' views on electronic data sharing for healthcare and research. J Am Med Inform Assoc JAMIA Jul. 2015;22(4):821–30. https://doi.org/10.1093/jamia/ocv014.
[15] Pool J, Akhlaghpour S, Fatehi F. Towards a contextual theory of Mobile Health Data Protection (MHDP): a realist perspective. Int J Med Inf Sep. 2020;141:104229. https://doi.org/10.1016/j.ijmedinf.2020.104229.
[16] Thoral PJ, et al. Sharing ICU patient data responsibly under the society of critical care medicine/European society of intensive care medicine joint data science collaboration: the Amsterdam university medical centers database (AmsterdamUMCdb) example. Crit Care Med Jun. 2021;49(6):e563–77. https://doi.org/10.1097/CCM.0000000000004916.
[17] Saksena N, Matthan R, Bhan A, Balsari S. Rebooting consent in the digital age: a governance framework for health data exchange. BMJ Glob Health Jul. 2021;6(Suppl 5):e005057. https://doi.org/10.1136/bmjgh-2021-005057.
[18] Kirkpatrick JP, et al. Implementing and integrating a clinically driven electronic medical record for radiation oncology in a large medical Enterprise. Front Oncol 2013;3. https://doi.org/10.3389/fonc.2013.00069.
[19] Tiwari B, Kumar A. Role-based access control through on-demand classification of electronic health record. Int J Electron Healthc 2015;8(1):9. https://doi.org/10.1504/IJEH.2015.071637.
[20] Anwar M, Imran A. Access control for multi-tenancy in cloud-based health information systems. In: 2015 IEEE 2nd international conference on cyber security and cloud computing. New York, NY: IEEE; Nov. 2015. https://doi.org/10.1109/CSCloud.2015.95.
[21] Jayabalan M, O'Daniel T. 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). Yogyakarta: IEEE; Nov. 2017. p. 165–70. https://doi.org/10.1109/ICITISEE.2017.8285487.
[22] Amato F, De Pietro G, Esposito M, Mazzocca N. An integrated framework for securing semi-structured health records. Knowl-Based Syst May 2015;79:99–117. https://doi.org/10.1016/j.knosys.2015.02.004.
[23] Sun L, Yong J, Soar J. Access control management for e-Healthcare in cloud environment. ICST Trans Scalable Inf Syst Mar. 2014;1(2):e3. https://doi.org/10.4108/sis.1.2.e3.
[24] Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A. Security and privacy in electronic health records: a systematic literature review. J Biomed Inf Jun. 2013;46(3):541–62. https://doi.org/10.1016/j.jbi.2012.12.003.
[25] Jayabalan M, O'Daniel T. Access control and privilege management in electronic health record: a systematic literature review. J Med Syst Dec. 2016;40(12):261. https://doi.org/10.1007/s10916-016-0589-z.
[26] Deane AJ, Kraus A. The official (ISC)2 CISSP CBK reference. sixth ed. Hoboken, New Jersey: John Wiley & Sons, Inc.; 2021.
[27] Tsegaye T, Flowerday S. A Clark-Wilson and ANSI role-based access control model. Inf Comput Secur Jun. 2020;28(3):373–95. https://doi.org/10.1108/ICS-08-2019-0100.
[28] Khamadja S, Adi K, Logrippo L. Designing flexible access control models for the cloud. In: Proceedings of the 6th international conference on security of information and networks. Aksaray Turkey: ACM, Nov.; 2013. p. 225–32. https://doi.org/10.1145/2523514.2527005.
[29] Guo B, Shukor NSA, Ishak IS. Enhancing healthcare services through cloud service: a systematic review. Int J Electr Comput Eng IJECE Feb. 2024;14(1):1135. https://doi.org/10.11591/ijece.v14i1.pp1135-1146.
[30] Vegh L. Cyber-physical systems security through multi-factor authentication and data analytics. In: 2018 IEEE international conference on industrial technology (ICIT); Feb. 2018. p. 1369–74. https://doi.org/10.1109/ICIT.2018.8352379.
[31] Liu W, Liu X, Liu J, Wu Q, Zhang J, Li Y. Auditing and revocation enabled role-based access control over outsourced private EHRs. In: 2015 IEEE 17th international conference on high performance computing and communications, 2015 IEEE 7th international symposium on cyberspace safety and security, and 2015 IEEE 12th international conference on embedded software and systems. New York, NY: IEEE; Aug. 2015. p. 336–41. https://doi.org/10.1109/HPCC-CSS-ICESS.2015.10.
[32] Calvillo-Arbizu J, Roman-Martinez I, Roa-Romero LM. Standardized access control mechanisms for protecting ISO 13606-based electronic health record systems. In: IEEE-EMBS international conference on biomedical and health informatics (BHI). Valencia, Spain: IEEE; Jun. 2014. p. 539–42. https://doi.org/10.1109/BHI.2014.6864421.
[33] Bhartiya S, Mehrotra D, Girdhar A. Proposing hierarchy-similarity based access control framework: a multilevel Electronic Health Record data sharing approach for interoperable environment. J King Saud Univ - Comput Inf Sci Oct. 2017;29(4):505–19. https://doi.org/10.1016/j.jksuci.2015.08.005.
[34] Sicuranza M, Esposito A. An Access Control Model for easy management of patient privacy in EHR systems. Presented at the 8th international conference for internet technology and secured transactions (ICITST-2013). London, UK: IEEE; 2014. https://doi.org/10.1109/ICITST.2013.6750243.
[35] De Oliveira MT, Verginadis Y, Reis LHA, Psarra E, Patiniotakis I, Olabarriaga SD. AC-ABAC: attribute-based access control for electronic medical records during acute care. Expert Syst Appl Mar. 2023;213:119271. https://doi.org/10.1016/j.eswa.2022.119271.
[36] Rivera Sánchez YK, Demurjian SA, Baihan MS. A service-based RBAC & MAC approach incorporated into the FHIR standard. Digit Commun Netw Nov. 2019;5(4):214–25. https://doi.org/10.1016/j.dcan.2019.10.004.
[37] Abomhara M, Yang H, Køien GM, Lazreg MB. Work-based access control model for cooperative healthcare environments: formal specification and verification. J Healthc Inform Res Jun. 2017;1(1):19–51. https://doi.org/10.1007/s41666-017-0004-7.
[38] Singh A, Chatterjee K. Trust based access control model for securing electronic healthcare system. J Ambient Intell Hum Comput Nov. 2019;10(11):4547–65. https://doi.org/10.1007/s12652-018-1138-z.
[39] Wollard KK, Shuck B. Antecedents to employee engagement: a structured review of the literature. Adv Develop Hum Resour Nov. 2011;13(4):429–46. https://doi.org/10.1177/1523422311431220.
[40] Nakano D, Muniz Jr J. Writing the literature review for empirical papers. Production Mar. 2018;28(0). https://doi.org/10.1590/0103-6513.20170086.
[41] Rewhorn S. Writing your successful literature review. J Geogr High Educ 2017. https://doi.org/10.1080/03098265.2017.1337732.
[42] Knopf JW. "Doing a literature review," PS polit. Sci Pol 2006;39(1):127–32. https://doi.org/10.1017/S1049096506060264.
[43] De Carvalho Junior MA, Bandiera-Paiva P. Health information system role-based access control current security trends and challenges. J Healthc Eng 2018;2018:1–8. https://doi.org/10.1155/2018/6510249.
[44] Liberati A, et al. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. J Clin Epidemiol Oct. 2009;62(10):e1–34. https://doi.org/10.1016/j.jclinepi.2009.06.006.
[45] Arsad FS, et al. The impact of eHealth applications in healthcare intervention: a systematic review. J Health Res Aug. 2022;37(3):178–89. https://doi.org/10.56808/2586-940X.1020.
[46] Guo H, Li W, Nejad M, Shen C-C. Access control for electronic health records with hybrid blockchain-edge architecture. In: 2019 IEEE international conference on blockchain (blockchain). Atlanta, GA, USA: IEEE; Jul. 2019. p. 44–51. https://doi.org/10.1109/Blockchain.2019.00015.
[47] De Oliveira MT, Dang H-V, Reis LHA, Marquering HA, Olabarriaga SD. AC-AC: dynamic revocable access control for acute care teams to access medical records. Smart Health Apr. 2021;20:100190. https://doi.org/10.1016/j.smhl.2021.100190.
[48] Seol K, Kim Y-G, Lee E, Seo Y-D, Baik D-K. Privacy-Preserving attribute-based access control model for XML-based electronic health record system. IEEE Access 2018;6:9114–28. https://doi.org/10.1109/ACCESS.2018.2800288.
[49] Guo C, Zhuang R, Jie Y, Ren Y, Wu T, Choo K-KR. Fine-grained database field search using attribute-based encryption for E-healthcare clouds. J Med Syst Nov. 2016;40(11):235. https://doi.org/10.1007/s10916-016-0588-0.
[50] Zhang A, Bacchus A, Lin X. Consent-based access control for secure and privacy-preserving health information exchange. Secur Commun Network Nov. 2016;9(16):3496–508. https://doi.org/10.1002/sec.1556.
[51] Sicuranza M, Esposito A, Ciampi M. An access control model to minimize the data exchange in the information retrieval. J Ambient Intell Hum Comput Dec. 2015;6(6):741–52. https://doi.org/10.1007/s12652-015-0275-x.
[52] Zhang X, Poslad S, Ma Z. Block-based access control for blockchain-based electronic medical records (EMRs) query in eHealth. In: 2018 IEEE global

communications conference (GLOBECOM). Abu Dhabi, United Arab Emirates: IEEE; Dec. 2018. p. 1–7. https://doi.org/10.1109/GLOCOM.2018.8647433.
[53] Saini A, Zhu Q, Singh N, Xiang Y, Gao L, Zhang Y. A smart-contract-based access control framework for cloud smart healthcare system. IEEE Internet Things J Apr. 2021;8(7):5914–25. https://doi.org/10.1109/JIOT.2020.3032997.
[54] Smithamol MB, Rajeswari S. Hybrid solution for privacy-preserving access control for healthcare data. Adv Electr Comput Eng 2017;17(2):31–8. https://doi.org/10.4316/AECE.2017.02005.
[55] Zhao F, Yu J, Yan B. Towards cross-chain access control model for medical data sharing. Procedia Comput Sci 2022;202:330–5. https://doi.org/10.1016/j.procs.2022.04.045.
[56] Gardiyawasam Pussewalage HS, Oleshchuk VA. Attribute based access control scheme with controlled access delegation for collaborative E-health environments. J Inf Secur Appl Dec. 2017;37:50–64. https://doi.org/10.1016/j.jisa.2017.10.004.
[57] Mhatre S, Nimkar AV. Secure cloud-based federation for EHR using multi-authority ABE. In: Panigrahi CR, Pujari AK, Misra S, Pati B, Li K-C, editors. Progress in advanced computing and intelligent engineering. Advances in intelligent systems and computing, 714. Singapore: Springer Singapore; 2019. p. 3–15. https://doi.org/10.1007/978-981-13-0224-4_1. 714.
[58] Chinnasamy P, Deepalakshmi P. HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. J Ambient Intell Hum Comput Feb. 2022;13(2):1001–19. https://doi.org/10.1007/s12652-021-02942-2.
[59] Psarra E, Apostolou D, Verginadis Y, Patiniotakis I, Mentzas G. Context-based, predictive access control to electronic health records. Electronics Sep. 2022;11(19):3040. https://doi.org/10.3390/electronics11193040.
[60] Guesmia K, Boustia N. OrBAC from access control model to access usage model. Appl Intell Aug. 2018;48(8):1996–2016. https://doi.org/10.1007/s10489-017-1064-3.
[61] Lo N-W, Wu C-Y, Chuang Y-H. An authentication and authorization mechanism for long-term electronic health records management. Procedia Comput Sci 2017;111:145–53. https://doi.org/10.1016/j.procs.2017.06.021.
[62] Feng Q, He D, Wang H, Zhou L, Choo K-KR. Lightweight collaborative authentication with key protection for smart electronic health record system. IEEE Sensor J Feb. 2020;20(4):2181–96. https://doi.org/10.1109/JSEN.2019.2949717.
[63] Samadbeik M, Gorzin Z, Khoshkam M, Roudbari M. Managing the security of nursing data in the electronic health record. Acta Inf Med Feb. 2015;23(1):39–43. https://doi.org/10.5455/aim.2015.23.39-43.
[64] Soceanu A, Vasylenko M, Egner A, Muntean T. Managing the privacy and security of eHealth data. In: 2015 20th international conference on control systems and computer science. Bucharest, Romania: IEEE; May 2015. p. 439–46. https://doi.org/10.1109/CSCS.2015.76.
[65] Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. J Med Syst Aug. 2017;41(8):127. https://doi.org/10.1007/s10916-017-0778-4.
[66] Rezaeibagha F, Win KT, Susilo W. A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Inf Manag J Oct. 2015;44(3):23–38. https://doi.org/10.1177/183335831504400304.
[67] Bhandari P. "Triangulation in research | Guide, types, examples," scribbr [Online]. Available: https://www.scribbr.com/methodology/triangulation/. [Accessed 8 November 2023].
[68] Yeng PK, Nweke LO, Yang B, Ali Fauzi M, Snekkenes EA. Artificial intelligence–based framework for analyzing health care staff security practice: mapping review and simulation study. JMIR Med Inf Dec. 2021;9(12):e19250. https://doi.org/10.2196/19250.
[69] Damon F, Coetzee M. Towards a generic Identity and Access Assurance model by component analysis - a conceptual review. In: Proceedings of the first international conference on Enterprise systems: es 2013. Cape Town, South Africa: IEEE; Nov. 2013. p. 1–11. https://doi.org/10.1109/ES.2013.6690086.
[70] International Organization for Standardization. ISO/IEC 27002:2022 - information security, cybersecurity and privacy protection - information security controls. 2022. https://doi.org/10.3403/30390395.
[71] Kannelønning K, Katsikas SK. A systematic literature review of how cybersecurity-related behavior has been assessed. Inf Comput Secur Oct. 2023;31(4):463–77. https://doi.org/10.1108/ICS-08-2022-0139.
[72] Sonkamble RG, Phansalkar SP, Potdar VM, Bongale AM. Survey of interoperability in electronic health records management and proposed blockchain based framework: MyBlockEHR. IEEE Access 2021;9:158367–401. https://doi.org/10.1109/ACCESS.2021.3129284.
[73] D. Jansen, "Qualitative Data Coding 101 (With Examples)," Grad Coach. Accessed: December. 15, 2023. [Online]. Available: https://gradcoach.com/qualitative-data-coding-101/.
[74] Whitman ME, Mattord HJ. Principles of information security. fourth ed. 20 2014. Channel Center, Boston, MA 02210, USA: Course Technology.
[75] Jaiman V, Urovi V. A consent model for blockchain-based health data sharing platforms. IEEE Access 2020;8:143734–45. https://doi.org/10.1109/ACCESS.2020.3014565.
[76] Kanwal T, Anjum A, Malik SUR, Khan A, Khan MA. Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud. Comput Stand Interfac Oct. 2021;78:103522. https://doi.org/10.1016/j.csi.2021.103522.
[77] Mohamad Jawad HH, Bin Hassan Z, Zaidan BB, Mohammed Jawad FH, Mohamed Jawad DH, Alredany WHD. A systematic literature review of enabling IoT in healthcare: motivations, challenges, and recommendations. Electronics 2022;11(19). https://doi.org/10.3390/electronics11193223.
[78] Schreuders ZC, McGill T, Payne C. The state of the art of application restrictions and sandboxes: a survey of application-oriented access controls and their shortfalls. Comput Secur Feb. 2013;32:219–41. https://doi.org/10.1016/j.cose.2012.09.007.
[79] Lacson JJ, et al. Smart city assessment in developing economies: a scoping review. Smart Cities Aug. 2023;6(4). https://doi.org/10.3390/smartcities6040081. , Art. no. 4.
[80] Briere J-B, Bowrin K, Taieb V, Millier A, Toumi M, Coleman C. Meta-analyses using real-world data to generate clinical and epidemiological evidence: a systematic literature review of existing recommendations. Curr Med Res Opin Dec. 2018;34(12):2125–30. https://doi.org/10.1080/03007995.2018.1524751.
[81] Levy BD, et al. Future research directions in asthma. An NHLBI working group report. Am J Respir Crit Care Med Dec. 2015;192(11):1366–72. https://doi.org/10.1164/rccm.201505-0963WS.
[82] Labaree RV. Research guides: organizing your social sciences research paper: 9. The conclusion [Online]. Available: https://libguides.usc.edu/writingguide/conclusion. [Accessed 14 April 2024].
[83] Community College of Denver. Writing an effective conclusion [Online]. Available: https://www.ccd.edu/download/file/fid/13985. [Accessed 20 December 2023].
[84] Ross PT, Bibler Zaidi NL. Limited by our limitations | perspectives on medical education. Perspect Med Educ Jul. 2019. https://doi.org/10.1007/s40037-019-00530-x.
[85] Labaree RV. Research guides: organizing your social sciences research paper: limitations of the study [Online]. Available: https://libguides.usc.edu/writingguide/limitations. [Accessed 14 April 2024].
[86] Bezet A. LibGuides: research process: literature gap and future research [Online]. Available: https://resources.nu.edu/researchprocess/literaturegap. [Accessed 14 April 2024].
[87] Velarde K, et al. Virtual surgical planning in craniomaxillofacial surgery: a structured review. Comput Assist Surg Abingdon Engl Dec. 2023;28(1):2271160. https://doi.org/10.1080/24699322.2023.2271160.
[88] Gardiyawasam Pussewalage HS, Oleshchuk VA. Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. Int J Inf Manag Dec. 2016;36(6):1161–73. https://doi.org/10.1016/j.ijinfomgt.2016.07.006.
[89] Shreyas S. Security model for cloud computing: case report of organizational vulnerability. J Inf Secur 2023;14(4):250–63. https://doi.org/10.4236/jis.2023.144015.
[90] Tipton SJ, Forkey S, Choi YB. Toward proper authentication methods in electronic medical record access compliant to HIPAA and C.I.A. Triangle. J Med Syst Apr. 2016;40(4):100. https://doi.org/10.1007/s10916-016-0465-x.
[91] Watzlaf VJM, Zhou L, DeAlmeida DR, Hartman LM. A systematic review of research studies examining telehealth privacy and security practices used by healthcare providers. Int J Telerehabilitation Nov. 2017;9(2):39–58. https://doi.org/10.5195/ijt.2017.6231.
[92] Chenchev I, Aleksieva-Petrova A, Petrov M. Authentication mechanisms and classification: a literature survey. In: Intelligent computing. Lecture notes in networks and systems, 3. Cham: Springer; 2021. p. 1051–70. https://doi.org/10.1007/978-3-030-80129-8_69. 1st ed., vol. 3.
[93] Arora S, Yttri J, Nilsen W. Privacy and security in mobile health (mHealth) research. Alcohol Res Curr Rev 2014;36(1):143–52.
[94] Tertulino R, Antunes N, Morais H. Privacy in electronic health records: a systematic mapping study. J Public Health Jan. 2023. https://doi.org/10.1007/s10389-022-01795-z.
[95] Sookhak M, Jabbarpour MR, Safa NS, Yu FR. Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues. J Netw Comput Appl Mar. 2021;178:102950. https://doi.org/10.1016/j.jnca.2020.102950.
[96] Thapa C, Camtepe S. Precision health data: requirements, challenges and existing techniques for data security and privacy. Comput Biol Med Feb. 2021;129:104130. https://doi.org/10.1016/j.compbiomed.2020.104130.
[97] Forcier MB, Gallois H, Mullan S, Joly Y. Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers? J Law Biosci Oct. 2019;6(1):317–35. https://doi.org/10.1093/jlb/lsz013.
[98] Politou E, Alepis E, Patsakis C. Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions. J Cybersecurity Jan. 2018;4(1). https://doi.org/10.1093/cybsec/tyy001.
[99] Asghar MR, Lee T, Baig MM, Ullah E, Russello G, Dobbie G. A review of privacy and consent management in healthcare: a focus on emerging data sources. In: 2017 IEEE 13th International Conference on e-Science (e-Science); Oct. 2017. p. 518–22. https://doi.org/10.1109/eScience.2017.84.
[100] Adler-Milstein J, Adelman JS, Tai-Seale M, Patel VL, Dymek C. EHR audit logs: a new goldmine for health services research? J Biomed Inf Jan. 2020;101:103343. https://doi.org/10.1016/j.jbi.2019.103343.
[101] Rule A, Chiang MF, Hribar MR. Using electronic health record audit logs to study clinical activity: a systematic review of aims, measures, and methods. J Am Med Inf Assoc Mar. 2020;27(3):480–90. https://doi.org/10.1093/jamia/ocz196.
[102] Kiourtis A, Mavrogiorgou A, Vidakis K, Kyriazis D. Health record index: secure access of cloud-stored healthcare data. In: The importance of health informatics in

public health during a pandemic. IOS Press; 2020. p. 221–4. https://doi.org/10.3233/SHTI200534.

[103] Suryawanshi K, Narkhede S. Green ICT for sustainable development: a higher education perspective. Procedia Comput Sci Jan. 2015;70:701–7. https://doi.org/10.1016/j.procs.2015.10.107.

[104] Karabetian A, et al. An environmentally-sustainable dimensioning workbench towards dynamic resource allocation in cloud-computing environments. In: 2022 13th international conference on information, intelligence, systems & applications (IISA); 2022. p. 1–4. https://doi.org/10.1109/IISA56318.2022.9904367.