Multicriteria Algorithms with Applications

Journal Homepage: sciencesforce.com/mawa

Multicriteria Algo. Appl. Vol. 3 (2024) 32–41

Paper Type: Review Article

Privacy Issues in Electronic Medical Records: A Systematic Review

Ahed J Alkhatib [1,*], Areej AlZoubi [2], Ahmad AlAiad [3], Aseel Abu Aqoulah [4], Almo'men Bellah Alawnah [5], Mohamad Alharoun [6], and Moe'en Azar [7]

[1] Legal Medicine, Toxicology of Forensic Science and Toxicology Department, Jordan University of Science and Technology; ajalkhatib@just.edu.jo.

[2] Computer Information Systems Department, Jordan University of Science and Technology; azalzoubi19@cit.just.edu.jo.

[3] Computer Information Systems Department, Jordan University of Science and Technology; aiaiad@just.edu.jo.

[4] Health Services Administration Department, Yarmouk University; 2020162027@ses.yu.edu.jo.

[5] Industrial Engineering Department, Jordan University of Science and Technology; akalawanah19@eng.just.edu.jo.

[6] Medical Laboratory Sciences Department, Hashemite University; mhmdharon996@gmail.com.

[7] Renewable Energy Engineering Sustainable Development Department, Jordan University of Science and Technology; mrazar986@bau.edu.jo.

Received: 02 Nov 2023 **Revised:** 11 Feb 2024 **Accepted:** 09 Mar 2024 **Published:** 13 Mar 2024

Abstract

Background: Recently, there has been a great development in healthcare services, and in the future, it is expected to evolve even more. The incorporation of the latest technologies, such as modern sensors, networks and cloud computing, has revolutionized the traditional healthcare system, one of the most important of these Updates electronic medical records that are a substitute for paper records. **Objectives:** This paper presents a systematic study of the recent literature on privacy issues faced by electronic medical records (EMR), through which we provide a comprehensive review, analysis and synthesis of research published in the past five years. **Methodology:** We collected relevant literature published between 2016 and 2021 and reviewed the approved issues, research problems, manuscript scopes, research methodologies, and main findings. 29 studies yielded our final extracted cohort. **Conclusions:** Using the objective analysis of the extracted cohort, we present a research typology that summarizes the major EMR privacy issues of relevant recent research in this field.

Keywords: Privacy, Electronic Medical Records, EMR, Issues.

1 | Introduction

Recently, there has been a great development in healthcare services, and in the future, it is expected to evolve even more. The incorporation of the latest technologies, such as modern sensors, networks and cloud computing, has revolutionized the traditional healthcare system, one of the most important of these Updates electronic medical records that are a substitute for paper records.

Corresponding Author: ajalkhatib@just.edu.jo

https://doi.org/10.61356/j.mawa.2024.311761

Electronic medical records (EMR) systems are electronic records that contain health information associated with patients who attend medical institutions and clinics for the purpose of treatment for various diseases. These records are created and managed by patients, physicians, and authorized personnel within medical institutions and clinics, and these records provide many benefits to patients, physicians, medical institutions, and clinics [1]. Electronic medical records can facilitate the workflow process and improve the quality of medical services provided to patients. Despite these benefits, there are, in turn, some negatives and fears from the adoption of these medical records, especially by patients, and the lack of mastery of their use by doctors and health care providers [2].

In view of the benefits of electronic medical records in the health care process, in 2003 the Institute of Medicine issued eight major functions that must be provided by electronic medical records.

1. The ability of the doctor to access various patient information.
2. The ability to access the results of new and previous examinations.
3. The ability to enter an electronic provider request.
4. Electronic decision support systems.
5. The ability to communicate electronically between doctors and patients.
6. A patient's ability to access electronic health records.
7. Introducing electronic management.
8. The ability to store electronic data.

Electronic medical records have developed rapidly in line with the development of technology around the world, and this would create a gap and ethical challenges associated with the use of electronic medical records [3], including privacy and data protection [4-7].

It is critical to implement electronic medical records in any country in the world to promote an excellent healthcare delivery system. To fully enjoy electronic medical records services, it is very important and necessary to put in place the required security and privacy mechanisms to prevent any form of security breach and vulnerability. We were able to review the literature on the security and privacy of electronic medical records and identify issues in current systems, in order to have an effective solution for electronic medical records.

In this study we aim to answer the following research questions:

RQ1: What are the gaps in the current EMR?

RQ2: What issues of privacy and security currently exist in EMR?

To answer the research questions above, we conducted a systematic review of the literature to determine the research papers concerned with EMR. To reach this goal, we followed the methodology of reviewing the systematic literature proposed by [8], and [9] in their methodology. The systematic review process consists of three stages: planning for the systematic review, conducting a systematic review, and extracting and synthesizing data.

As a result of this systematic review, it consisted of answers to questions about EMR, and what issues remained unresolved and need further research. We also highlight and focus on the main restrictions of current EMR to guide future research by providing a road map and a set of new research questions.

The results of this systematic multi-dimensional review will enable researchers, academics and technologists in the field of healthcare to understand research guide their path in future research in this field, we suggest a classification in which we present the issues of privacy and security.

2 | Related Work

In this study [10], the authors examined the Health Insurance Transfer and Accountability Act (HIPAA) of 1996 to reveal its impact on the functioning of health institutions. It turns out that the HIPAA system contains five complex addresses. However, aspects of the known HIPAA are the privacy ones for electronic medical records. HIPAA provides a set of Protected Health Information (PHI) databases and information that is most in need of protection. HIPAA offers the privacy and protection of the privacy of health information in electronic health records.

In this paper [11], the authors' goal was to verify the security and privacy of electronic health care records, so they identified the basic components of electronic health records: health data, medical devices, medical networks, and the cloud. The authors reviewed literature looking at the privacy of EHRs concerned with each component of the EHR. The results we obtained are search rankings, security concerns, requirements, solutions, research trends, and challenges for components with strengths and weaknesses.

The aim of this study [12] was to review relevant research to reveal the most important ethical, legal, and social issues when research uses electronic health records for individuals with intellectual disabilities. The authors reviewed relevant research to reveal issues associated with the use of electronic health records. This review resulted in 59 papers that summarize the following: informed consent, privacy and security, return outcomes, and vulnerable populations.

The aim of this research [13] was to compare the policies and infrastructures of healthcare information technology for two countries: the United States and the United Kingdom. The paper focuses on electronic health record (EHR) systems, and the security and privacy of health care information. The authors did a review of the health care literature. It was found that despite the increasing use of electronic health records in the United States and the United Kingdom, the two countries face significant obstacles in the operation of electronic health record systems in the country. To ensure patient safety, operational standards that ensure easy communication between different systems and appropriate security and privacy orders for data collection, data processing and data sharing.

In this paper [14], the authors provide a systematic literature review of blockchain approaches to electronic health records, focusing on security and privacy issues. The authors provide basic knowledge associated with electronic health records and the blockchain. Blockchain has demonstrated tremendous capabilities in the development of traditional healthcare.

3 | Research Methodology

Systematic review process according to the research methodology in [15, 16]. Figure 1 shows the three stages of the methodology and its steps. The planning process of the review was aimed at defining the research goals and the expected results. In this study, we have reviewed published articles about the issues of EMR; we have also developed a thematic classification for research and provided guidance for future research in this field.

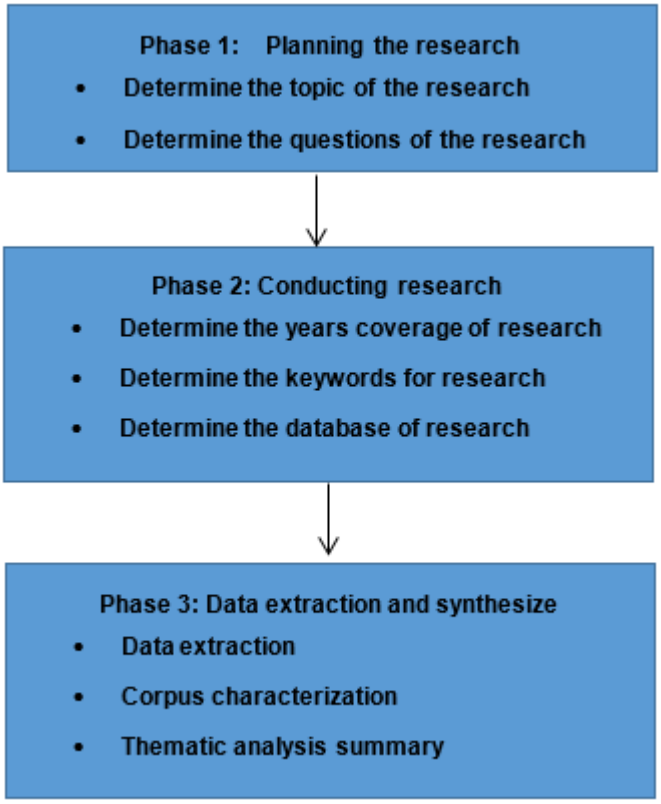

Figure 1. Stages of the methodology and its steps.

Our aim from the second stage, conducting the review, was to conduct a comprehensive search of all research results and unbiased literature, based on many research rules, to define a set of articles to be reviewed. These rules include specifying the keywords that will be used to search for articles and specifying the databases to search for. We decided to research three of the most well-known and quality databases in health informatics: PubMed, ScienceDirect, and Google scholar. The extent of years of publication has been determined to be covered; we targeted research published between 2016 and 2021.

Then, we defined search terms and keywords were initially selected based on research and included the privacy in electronic medical records. During this initial search, we noticed that the basic concept of research has multiple synonyms in different databases because the names differ, some researchers use the term electronic medical records, and others use the term EMR. Therefore, to ensure that we will obtain an accurate and comprehensive list of papers related to our issues from the mentioned databases, we have arranged search terms and keywords in several different search strings that can operate on all databases. We compiled the outputs of this search into an Excel spreadsheet, to give an initial set of 2236 published workbooks used for further analysis as shown in Figure 2. In the next stage, we defined and formulated the criteria for inclusion and exclusion. We reached the following criteria:

i. The set of documents should only include studies published in the English language.

ii. The group should also include research articles and conference proceedings.

iii. We have reviewed titles and summaries using our selection rules related to the content.

iv. We reviewed the full text using our selection rules related to the content, and 29 articles and procedure papers were used for further analysis by extracting data.

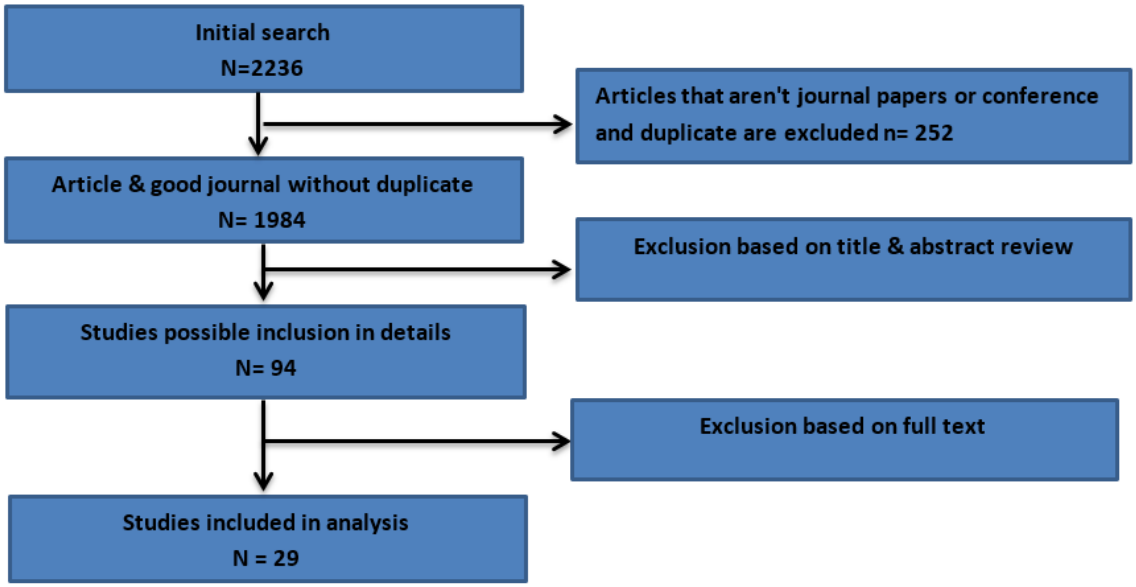

Figure 2. Number of articles in each stage based on inclusion and exclusion criteria.

We conducted the research selection process and at the end of this process, we found 29 research articles that meet the search criteria that we set, through which we will try to find the answer to our research questions. Then, we moved on to extracting data for synthesis. The main goal of the data extraction process was to examine the elements in the final group that serve our research goals and research questions and record the features of their interest. The goal of data synthesis is to make a summary of the articles we have come up with, extract the results we need, and combine them to reach our goals.

4 | Results

After selecting a group of 29 articles based on the inclusion and exclusion criteria mentioned above, we moved to extracting and synthesizing data, to achieve the goal of this research and to provide answers to the research questions.

Data extraction we collected a set of 29 articles to extract the data. Emphasis was placed on the research problem and objectives. Data extraction helped us conduct an in-depth review of current research to answer research questions correctly and clearly, the articles were reviewed separately. The selected studies were published in our group between 2016 and 2021.

Thematic analysis summary based on the thematic analysis of 29 article studies, we identified seven issues of privacy of EMR. Using the aggregate narration approach, we provided a brief description of each theme. Below is a summary of the main results for each issue:

4.1 | Breaches Data, Cyber-Attacks

With the technological progress in the field of health care and the use of the Internet to provide service and care for patients, it is better to publish electronic health records services via the cloud, but there are issues and problems related to the security and privacy of health data, and the spread of the problem of data penetration has made sharing health data practical Difficult.

It is worth noting some of the various data breaches, including health data, such as Denial of Service (DoS) attacks, collusion attacks, spoofing, man-in-middle attacks, and cloud malware injection attacks [14/13sch]. There are many requirements to ensure the security and privacy of health data, such as the Health Insurance Portability and Accountability Act (HIPAA).

One of the services provided by electronic medical records is the immediate query and request an exchange of data, but it leads to the problem of the unauthorized use, access, and disclosure of patients' private data, and this creates problems related to the security and privacy of patients.

4.2 | Privacy Protection

The concept of patient privacy is a dynamic and sensitive one that is clear and consistent with privacy issues across studies. There is a contradiction that makes it difficult to describe patients' requirements for privacy. The fear of privacy has decreased since 2010, particularly in the use of Protected Health Data [3sec]. This indicator directs us to the question of how the concept of privacy of health data in patients might change.

Therefore, the focus could be on protecting personal privacy in electronic medical records. However, patients' requirements for privacy cannot be met using simple methods such as anonymization or security protocols.

4.3 | Unauthorized Access

Query and exchange of health data from electronic medical records to improve medical services, but it creates opportunities for unauthorized use of patient data, affecting the security and privacy of electronic medical records. Unauthorized use can have an impact on patients' families if their genetic data is included in the records. With electronic medical records, data transmission can easily cause records infringement. Violations may occur due to errors in the professional conduct of those authorized to use the records, such as inquiring about the results of examinations for a family member. Strict usage restriction policies in controlling access to private data can help maintain privacy.

4.4 | Trust

The Trust has an important role in increasing the effectiveness of electronic medical records while maintaining data where it is trustworthy and ensures an easy workflow. Meeting the requirements of security and privacy leads to creating and increasing the confidence of patients, doctors and others who use electronic medical records, and this leads to the success of these records and achieving the goal of using them instead of paper records.

4.5 | Personality Data

The biggest challenge in health care systems supported in the penetration or access to personal and sensitive data. Systems may be vulnerable to cyber-attacks and identity theft and personal data. To limit access to sensitive or personal data, it is better to encrypt personal data in the cloud, as this method can prevent access to this data. It is also possible to anonymize patients in electronic medical records, this method can ensure the privacy of patients' personal data, so that other data will not be usable for secondary use.

4.6 | Secondary Use

The use of electronic medical records creates privacy and security issues. The use of this data for secondary purposes threatens the privacy of electronic medical records. Electronic medical records enable healthcare providers to seamlessly access and share medical data. It is worth noting that the use of secondary electronic medical records and access to personal data affects the privacy of patients and electronic medical records.

4.7 | The Lack of Harmonized Policies and Common Standards Worldwide

The privacy and security of electronic medical records are one of the main issues facing the adoption of electronic medical records. Despite this, there are challenges in the implementation of electronic medical records for patients, and among these challenges is the lack of international policies and common standards between countries, and this creates a difficult challenge for security among medical organizations.

We have developed a classification of the most important issues related to the privacy of electronic medical records. Based on the issues studied by the most research described above, we have developed the classification of privacy issues (see Figure 3). There was no study that looked at all the issues facing the medical health records examined from 2016 to 2021. The objective of this classification is to provide a comprehensive reference model that helps researchers understand the focus of current issues.

To develop the classification, we first extracted seven major privacy issues for electronic medical records from the research cohort, as described previously. We grouped and categorized relevant and similar studies under one topic.

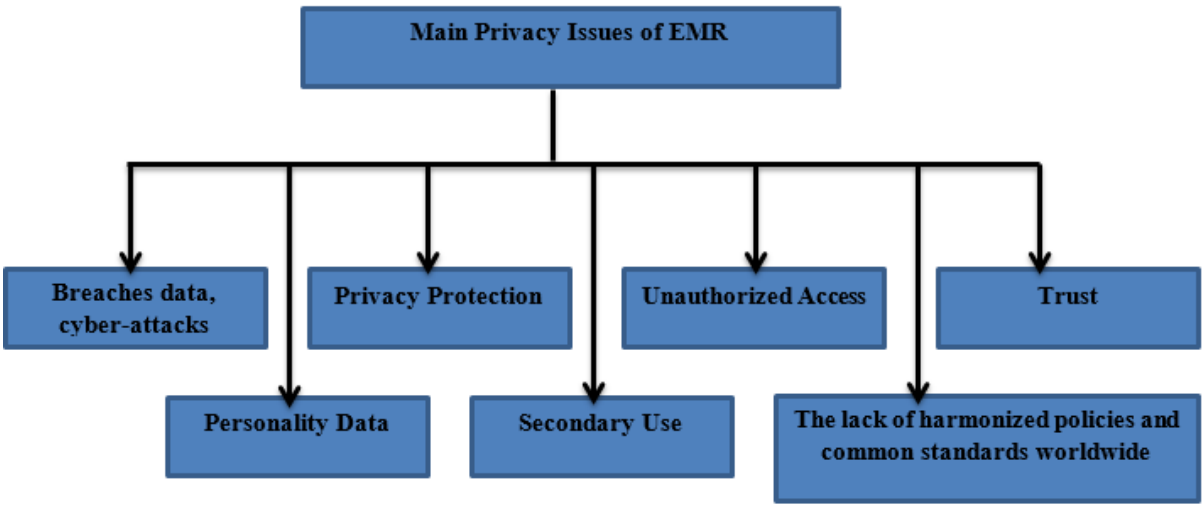

Figure 3. The main privacy issues of EMR.

In Table 1, we present a summary of the issues that have been studied through previous studies, with the special citation including the study that investigated this issue.

Table 1. Summary of privacy issues with papers.

Privacy Issues	Paper
Breaches data, cyber-attacks	[17][18][19][20] [21][22][23]
Privacy Protection	[24][25][26][27]
Unauthorized Access	[28][29][17][19][31][32]
Trust	[33] [34][35]
Personality Data	[3][36][37][38] [39]
Secondary Use	[30][40][41] [42]
The lack of harmonized policies and common standards worldwide	[43]

5 | Conclusion

The primary objective of our study was to perform a systematic review of the literature on EMR privacy issues in order to arrive at an answer to the research questions RQ1 and RQ2. This paper is an example of an application for a systematic literature review that guides future researchers in the privacy and security of electronic medical records. We objectively analyzed the current set of papers examining electronic medical record privacy issues and categorized seven major privacy issues, which were identified through this research together with the papers that were each studied. We believe that research and attention to these issues can

help provide more effective electronic medical record systems to provide appropriate medical care to patients. We suggest that there is a need for more research, regulations, and laws governing electronic medical records before they are issued to healthcare institutions in general to ensure their effectiveness in helping to provide health care services. We believe this work provides a major step forward in understanding the issues facing electronic medical records.

Acknowledgments

The author is grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

Author Contributaion

All authors contributed equally to this work.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] The National Alliance for Health Information Technology (NAHIT)

[2] L Sulmasy, A Lopez, ´ C. Horwitch, Ethical Implications of the Electronic Health Record: In the Service of the Patient, J. Gen. Intern. Med 32 (8) (2017) 935–939, https://doi.org/10.1007/s11606-017-4030-1. PMID: 28321550 PMCID: PMC5515784.

[3] Afzal, S., & Arshad, A. (2021). Ethical issues among healthcare workers using electronic medical records: A systematic review. *Computer Methods and Programs in Biomedicine Update*, *1*, 100030. https://doi.org/10.1016/j.cmpbup.2021.100030

[4] J Kulynych, HT. Greely, Clinical genomics, big data, and electronic medical records: reconciling patient rights with research when privacy and science collide, J. Law Biosci. 4 (1) (2017 Apr 1) 94–132, https://doi.org/10.1093/jlb/lsw061

[5] M Favaretto, D Shaw, E De Clercq, T Joda, BS. Elger, "Big data and digitalization in dentistry: a systematic review of the ethical issues", Int. J. Environ. Res. Public Health 17 (7) (2020 Jan2495), https://doi.org/10.3390/ijerph17072495

[6] I. Francis, "Using classical ethical principles to guide mHealth design", Online J. Issues Nurs. 21 (3) (2017 Nov 1).

[7] W Ricciardi, S. Boccia, "New challenges of public health: bringing the future of personalised healthcare into focus", Eur. J. Public Health 27 (suppl_4) (2017 Oct 1) 36–39, https://doi.org/10.1093/eurpub/ckx164, https://doi.org/.

[8] J. Ramey and P. G. Rao, "The systematic literature review as a research genre," in Proc. IEEE Int. Prof. Commun. Conf., 2011, pp. 1–7.

[9] P. G. Rao and J. Ramey, "Use of mobile phones by non-literate and semi-literate people: A systematic literature review," in Proc. IEEE Int. Prof. Commun. Conf., 2011, pp. 1–10.

[10] W. Moore and S. Frye, "Review of HIPAA, part 1: History, protected health information, and privacy and security rules," *Journal of Nuclear Medicine Technology*, vol. 47, no. 4, pp. 269–272, 2019.

[11] S.-R. Oh, Y.-D. Seo, and E. Lee, et al ,"A comprehensive survey on security and privacy for Electronic Health Data," *International Journal of Environmental Research and Public Health*, vol. 18, no. 18, p. 9668, 2021.

[12] M. Raspa, R. Moultrie, and L. Wagner, et al, "Ethical, legal, and social issues related to the inclusion of individuals with intellectual disabilities in Electronic Health Record Research: Scoping Review," *Journal of Medical Internet Research*, vol. 22, no. 5, 2020.

[13] K. Wilson and L. Khansa, "Migrating to Electronic Health Record Systems: A comparative study between the United States and the United Kingdom," *Health Policy*, vol. 122, no. 11, pp. 1232–1239, 2018.

[14] S. Shi, D. He, and L. Li, et al, "Applications of blockchain in ensuring the security and privacy of Electronic Health Record Systems: A survey," *Computers & Security*, vol. 97, p. 101966, 2020.

[15] J. Ramey and P. G. Rao, "The systematic literature review as a research genre," in Proc. IEEE Int. Prof. Commun. Conf., 2011, pp. 1–7.

[16] P. G. Rao and J. Ramey, "Use of mobile phones by non-literate and semi-literate people: A systematic literature review," in Proc. IEEE Int. Prof. Commun. Conf., 2011, pp. 1–10.

[17] L. S. Sulmasy and A. M. López, et al, "Ethical implications of the electronic health record: In the service of the patient," *Journal of General Internal Medicine*, vol. 32, no. 8, pp. 935–939, 2017.

[18] N. R. Anoop Bhola, "'blockchain based privacy preservation in Healthcare: A recent trends and challenges,"' *Psychology and Education Journal*, vol. 58, no. 1, pp. 5315–5324, 2021.

[19] Kamya Eria, "Security and Privacy of Health Data: A Review of the Challenges and Approaches,"' *Journal of Applied Technology and Innovation* (e-ISSN: 2600-7304) vol. 2, no. 2, (2018).

[20] N. A. Azeez and C. V. der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egyptian Informatics Journal*, vol. 20, no. 2, pp. 97–108, 2019.

[21] C. Thapa and S. Camtepe, "Precision Health Data: Requirements, challenges and existing techniques for data security and privacy," *Computers in Biology and Medicine*, vol. 129, p. 104130, 2021.

[22] K. Gariépy-Saper and N. Decarie, "Privacy of Electronic Health Records: A review of the literature," *Journal of the Canadian Health Libraries Association / Journal de l'Association des bibliothèques de la santé du Canada*, vol. 42, no. 1, 2021.

[23] OKEDIRAN, O. OA, " METHODICAL REVIEW OF SECURITY AND PRIVACY ISSUES IN CLOUD-BASED ELECTRONIC HEALTH RECORDS", *University of Pitesti Scientific Bulletin Series: Electronics and Computer Science*, *20*(1), 1-12. (2020).

[24] W. Sun, Z. Cai, and Y. Li, et al, "Data Processing and text mining technologies on Electronic Medical Records: A Review," *Journal of Healthcare Engineering*, vol. 2018, pp. 1–9, 2018.

[25] N. Shen, T. Bernier, and L. Sequeira, et al, "Understanding the patient privacy perspective on Health Information Exchange: A systematic review," *International Journal of Medical Informatics*, vol. 125, pp. 1–12, 2019.

[26] E. Chukwu and L. Garg, "A systematic review of Blockchain in Healthcare: Frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020.

[27] C. Thapa and S. Camtepe, "Precision Health Data: Requirements, challenges and existing techniques for data security and privacy," *Computers in Biology and Medicine*, vol. 129, p. 104130, 2021.

[28] C. S. Kruse, B. Smith, and H. Vanderlinden, "Security techniques for the Electronic Health Records," *Journal of Medical Systems*, vol. 41, no. 8, 2017.

[29] L. Kloss, M. Brodnik, and L. Rinehart-Thompson, "Access and disclosure of Personal Health Information: A challenging privacy landscape in 2016-2018," *Yearbook of Medical Informatics*, vol. 27, no. 01, pp. 060–066, 2018.

[30] I. Keshta and A. Odeh, "Security and privacy of Electronic Health Records: Concerns and challenges," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 177–183, 2021.

[31] A. A. Vazirani, O. O'Donoghue, and D. Brindley, et al, "Implementing blockchains for Efficient Health Care: Systematic Review," *Journal of Medical Internet Research*, vol. 21, no. 2, 2019.

[32] M. A. Sahi, H. Abbas, and K. Saleem, et al "Privacy preservation in e-healthcare environments: State of the art and Future Directions," *IEEE Access*, vol. 6, pp. 464–478, 2018.

[33] Abdulhameed, I. S ,"The Security and Privacy of Electronic Health Records in Healthcare Systems: A Systematic Review"., *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 1979-1992. 2021.

[34] F. N. Zulkipli, N. Hussin, and S. F. Yatin, "Critical success factor of trusted elements for Mobile Health Records Management: A review of conceptual models," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 9, 2021.

[35] A. H. Mayer, C. A. da Costa, and R. da Righi, "Electronic health records in a Blockchain: A systematic review," *Health Informatics Journal*, vol. 26, no. 2, pp. 1273–1288, 2019.

[36] Langarizadeh, M., Orooji, A., et al "Effectiveness of Anonymization Methods in Preserving Patients' Privacy: A Systematic Literature Review". *eHealth*, *248*, 80-87. 2018.

[37] Dias, A. A. M. R., & Pannala, U. K. "Security, Privacy and Confidentiality aspects of Healthcare Cloud Computing Systems: A Systematic Review".

[38] Limaa, V. C., Bernardia, F. A., Alvesc, D., & Lopes, R. P. C. "Security approaches for electronic health data handling through the Semantic Web: a scoping review".

[39] M. Tanriverdi, "A systematic review of privacy preserving healthcare data sharing on Blockchain," *Journal of Cybersecurity and Information Management*, pp. 31–37, 2020.

[40] S. M. Shah and R. A. Khan, "Secondary use of electronic health record: Opportunities and challenges," *IEEE Access*, vol. 8, pp. 136947–136965, 2020.

[41] M. Raspa, R. Moultrie, and L. Wagner, "Ethical, legal, and social issues related to the inclusion of individuals with intellectual disabilities in Electronic Health Record Research: Scoping Review," *Journal of Medical Internet Research*, vol. 22, no. 5, 2020.

[42] S. M. Shah and R. A. Khan, "Secondary use of electronic health record: Opportunities and challenges," *IEEE Access*, vol. 8, pp. 136947–136965, 2020.

[43] El Kettani, A., Housban, S., Serhier, Z., & Othmani, M. B. "Confidentiality in Electronic Health Records Systems: a Review". *Journal of Medical and Surgical Research*, *5*, 551-554. 2018.