MAESTRO: Management, Information Systems, Strategy & Operations
Volume 1, Number 1, 2026
P-ISSN: xxxx-xxxx E-ISSN : xxxx-xxxx
Open Access: https://maestro.com/

Mapping the Global Knowledge Structure of Electronic Medical Records and Data Security Research: A Hybrid Systematic Literature Review and Bibliometric Analysis

Dedi Risnandi
Universitas Esa Unggul, Jakarta, Indonesia
Correspondence: dedi.risnandi@student.esaunggul.ac.id

Article Info

Article history:
Received Nov 26th, 2025
Revised Des 31st, 2025
Accepted Jan 18th, 2026

Keyword:
Electronic Medical Record; Data Security; Systematic Literature Review; Bibliometric Analysis; Cybersecurity; Healthcare Governance

ABSTRACT

The rapid expansion of digital health services increased the use of electronic medical records, while simultaneously raising serious concerns regarding privacy and data protection. This study systematically mapped the global knowledge structure of electronic medical record and data security research to identify publication trends, thematic developments, and future research directions. A systematic literature review and bibliometric analysis were conducted using Scopus-indexed journal articles published between 2003 and 2025. The screening and eligibility process resulted in 86 relevant studies for analysis. The findings showed a strong growth of research after 2019, driven by accelerated digital transformation and increasing cybersecurity risks in healthcare systems. The intellectual landscape was dominated by three major themes: secure architectures using blockchain and encryption, governance and interoperability frameworks for health data management, and smart healthcare technologies enabling real-time clinical information exchange. Despite these advancements, persistent challenges remained related to regulatory harmonization, system interoperability, and user trust. Overall, this study provided a structured synthesis that supported future research and practical strategies for strengthening secure and resilient digital healthcare systems.

1. INTRODUCTION

The rapid growth of the digital health ecosystem has made the Electronic Medical Record (EMR) system a fundamental infrastructure for improving healthcare accessibility, clinical decision support, and operational efficiency (Greenhalgh et al., 2009; Yuan & Li, 2019). By facilitating the digitization of patient data and clinical processes, EMRs enhance patient care continuity and are a pillar of institutional data governance within each healthcare system (Greenhalgh et al., 2009; Wang et al., 2022). Nevertheless, the adoption of digital medical records has increased the risk of data breaches, unauthorized access, and privacy violations in cyberspace, turning data protection into a major issue for present healthcare (Fernández-Alemán et al., 2013; Rezaeibagha et al., 2015).

With the adoption of electronic medical records (EMRs) by health organizations, technological innovation is increasingly enmeshed with efficient data security protocols and regulatory frameworks such as the European Union’s GDPR and other national health information governance policies (Papadopoulos et al., 2025; Yuan & Li, 2019). Although research has been conducted in different scopes of EMR implementation and security solutions, there are fragmented views that address its technological, regulatory, and socio-technical aspects (Singh et al., 2024). As a result, there is a need for a systematic and integrated synthesis to understand the trends, topic concentration, and future research directions of EMR and data security, respectively. This gap is addressed in the present study using a hybrid of Systematic Literature Review and bibliometric analysis to map trends, orientations, and globalisation in knowledge structure on secure digital healthcare (Donthu et al., 2021; Papadopoulos et al., 2025)

This study tackles the following research questions: (1) In terms of publication growth, temporal trends, and overall research evolution, how has research into Electronic Medical Records (EMRs) and data security developed since 2003? (2) In this period, who are the most fertile and influential authors, institutions, and countries researching EMR and data security? (3) To what extent can the intellectual landscape of EMR and data security studies be defined? What are the major research themes, main research concerns, and future trends? (4) How have International research collaboration patterns developed within this research domain over time? (5) In light of healthcare data governance, interoperability, patient privacy, and in light of healthcare cybersecurity resilience, what new opportunities for further research have been discovered in current EMR research? By addressing these research issues, this paper aims to enhance the field of EMR data security research and to provide a basis for future scholarly inquiry and evidence-based policy in secure digital healthcare.

Rewriting helps establish an integrated perspective on Electronic Medical Record (EMR) and data security research that connects technological research with policy and security analysis. Indeed, such a combination enables the study to trace the interactive processes among digital health innovation, risk management in cyberspace, and the governance of healthcare data. This dual strategy allows for clearer graphing of global research trends and for tactical consequences for both academic research and practical policy-making. The findings lay a solid foundation for building a digital healthcare system that is not only resilient and secure but (in tune with 192) also ethically run.

2. LITERATURE REVIEW

According to the literature, electronic medical records (EMRs) are digital systems developed to manage patient health information within healthcare organizations (Liu et al., 2024; Wang et al., 2022). Furthermore, instead of being viewed merely as digital substitutes for paper-based records, earlier studies increasingly treat EMRs as an integral part of health information systems that support integrating data and clinical documentation as well as limitation-support processes (Goldberg et al., 2025; Halid & Binarto Budi Susilo, 2025; Shahzad et al., 2024). Changing healthcare systems in different countries of origin, including those that are still leading edge as well as underdeveloped ones, on the one hand emphasize EMRs' strategic posture vis-à -vis healthcare services and national e-health initiatives, but on the other hand consistently reveal tough challenges in interoperability (Ndlovu et al., 2021; Wang et al., 2022).

Within this body of research, data security and privacy emerge as recurring analytical concerns as sensitive medical information becomes increasingly centralized and transmitted digitally. Existing studies emphasize that inadequate safeguards may expose EMR systems to cyberattacks, unauthorized access, and data breaches, particularly in large-scale or resource-constrained environments (Kasim, 2022; Mishra et al., 2025). To mitigate these risks, the literature identifies encryption mechanisms, access control systems, authentication procedures, and user-permission policies as essential components of secure EMR management throughout the data lifecycle (Kasim, 2022; Kim et al., 2025). Regulatory compliance, including adherence to data protection frameworks such as the General Data Protection Regulation (GDPR), is also frequently discussed as a critical factor in strengthening patient trust and safeguarding confidentiality, especially for vulnerable and mobile populations (Tensen et al., 2025).

More recent studies are addressing EMR data security while examining next-generation digital solutions, such as blockchain-based solutions, that might address long-term challenges in trust and security. New researches in this field indicate the way blockchain can support decentralized data storages, unforgeable audit trails, stronger encryption in EMR applications (The healthier editing practices and safer cooperation between industry depending on healthcare information) (Han et al.,(Han et al., 2025; Pokharel et al., 2025). It also introduces such means as smart contracts and mixed storage architectures that can enable scalable access control and effective protection of critical medical records (Surasak, 2024; S. Zhu et al., 2025). But despite these technological developments, earlier studies are fragmented between the technical, organizational and regulatory perspectives. An integrative analysis is therefore needed to tie together old results from various fields of EMR, information security research, in a comprehensive manner that systematically maps its emerging intellectual structure and direction.

Table 1: Core Definitions of Electronic Medical Record and Data Security

No	Concept	Definition	Reference
1	Electronic Medical Record (EMR)	A digital version of a patient's paper-based medical record designed to support clinical documentation, diagnosis, and treatment within healthcare organizations.	(Liu et al., 2024)
2	Electronic Medical Record (EMR)	A core component of health information systems that replaces manual records and facilitates secure data integration across healthcare facilities.	(Halid & Binarto Budi Susilo, 2025)
3	Electronic Medical Record (EMR)	A structured digital repository that stores and manages patient health information, enabling efficient clinical workflows and decision support.	(Shahzad et al., 2024)
4	Data Security	The protection of digital health information from unauthorized access, breaches, corruption, or misuse throughout its lifecycle.	(D. Zhu et al., 2025)

Consistent with the literature review, it is theorized that Electronic Medical Records (EMRs) are digitized health information systems that allow the secure storage and management of patients' data in digital form and facilitate exchange across healthcare providers to support clinical decision-making and healthcare governance. The concept of data security in EMR systems is understood as a multidimensional construct that encompasses the use of technological measures and arrangements for governance and law compliance to prevent unauthorized access to information while also guaranteeing its confidentiality, integrity, notarization, availability, and reliability in the context of digital health devices.

3. METHODS AND ANALYSIS

This work has adopted a methodology that hybridizes a Systematic Literature Review (SLR) and bibliometric analysis to investigate the growth, intellectual structure, and research trends of studies on Electronic Medical Record (EMR) and data security. The review adhered to the revised PRISMA guidelines, which provide guidance on transparent reporting for identifying, screening, and inclusion of literature (Page et al., 2021). Related methods were adhered to for bibliometric and systematic review activities to ensure rigor and sustained consistency across all phases of inquiry (Donthu et al., 2021; Snyder, 2019).

3.1 Data Source and Search Strategy

This section describes the source and approach for selecting the data source, and our structured search strategy to locate literature on EMR and data security. We perform a literature search using the following string in Scopus: TITLE-ABS-KEY ("Electronic Medical Record" AND "Data Security") AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (OA , "all"))

In this case, the Scopus database was selected as the sole data source, as it encompasses a broad spectrum of knowledge areas and is suitable for systematic literature reviews and for reporting numerical outcomes in bibliometric analysis (Carrera-Rivera et al., 2022; Pranckutė, 2021). The final search string "Electronic Medical Record" AND "Data security" was executed across title, abstract, and author keywords, and the search was executed on October 12th, 2025. This search strategy was created to identify studies that mention EMRs and data protection separately.

3.2 Screening Process and PRISMA Flow

The first database search identified 5543 records published from 2003 to 2025. At the title and abstract screening stage, documents that did not mention both search terms were discarded, leaving 305 records potentially relevant. In the eligibility phase, references were categorized by document type, and peer-reviewed journal articles (n = 170) were screened in, and conference papers, review papers, book chapters, books, editorials, and notes were excluded. Next, non-English language publications were excluded articles in Chinese (n = 7), German (n = 5), Polish (n = 1), and Russian (n = 1), leaving 156 English-language journal articles. At the last stage of assessment, as well as full-text availability and metadata for compilation and bibliometric mapping of content they were used which resulted to a final sample of 86 journal articles data were included in this study. The study selection pipeline is summarized in Figure 1 in compliance with the PRISMA guidelines.

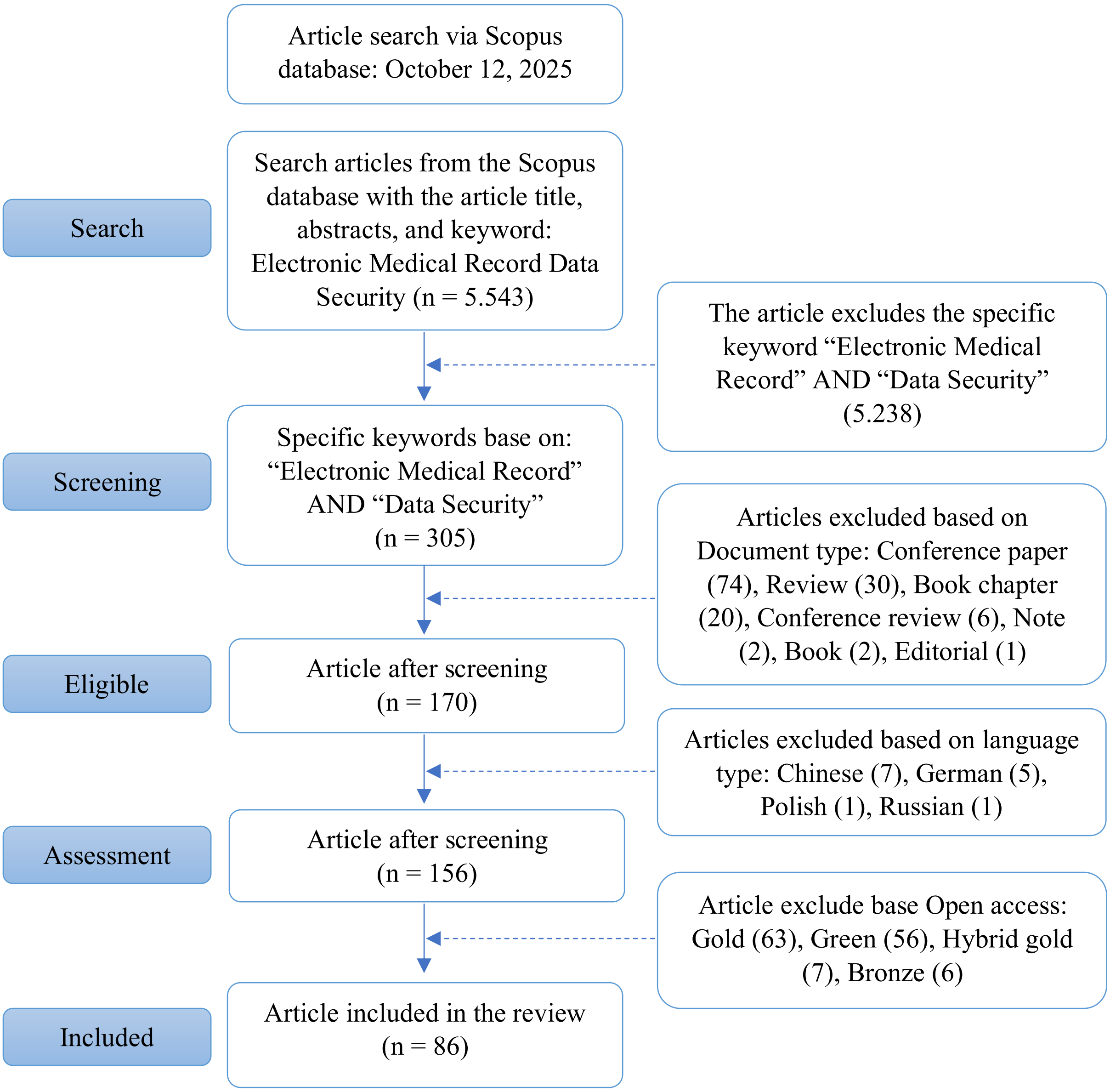
Article search via Scopus database: October 12, 2025
Search
Search articles from the Scopus database with the article title, abstracts, and keyword: Electronic Medical Record Data Security (n = 5.543)
The article excludes the specific keyword "Electronic Medical Record" AND "Data Security" (5.238)
Screening
Specific keywords base on: "Electronic Medical Record" AND "Data Security" (n = 305)
Articles excluded based on Document type: Conference paper (74), Review (30), Book chapter (20), Conference review (6), Note (2), Book (2), Editorial (1)
Eligible
Article after screening (n = 170)
Articles excluded based on language type: Chinese (7), German (5), Polish (1), Russian (1)
Assessment
Article after screening (n = 156)
Article exclude base Open access: Gold (63), Green (56), Hybrid gold (7), Bronze (6)
Included
Article included in the review (n = 86)

Figure 1: PRISMA flow diagram illustrating the study selection process

3.3 Inclusion and Exclusion Criteria

Peer-reviewed English-language journal articles published between 2003 and October 12, 2025 indexed in the Scopus database that directly discussed EMRs and data security within healthcare management and/or digital health or health information systems were included. Exclusion criteria were conference papers, books, book chapters, editorial articles, letters, review articles full texts that written in language other than English and studies not contained direct item related to EMR and Data Security.

3.4 Data Extraction and Synthesis

The bibliographical information, including publication year, author's identity, and institutional cites, was collected for every included article. This data substantiated both quantitative bibliometric mapping and the qualitative content synthesis to adverse thematic trends and research gaps. The main characteristics of the included studies are shown in Table 2.

3.5 Bibliometric Mapping and Visualization

Co-authorship networks, citation relations, and keyword co-occurrences were illustrated using the VOSviewer software for bibliometric analysis. The analysis was conducted on the bibliographic metadata downloaded from Scopus, which were centred around authors, institutions, countries and author keywords. Network representations were built to detect thematic clusters, collaboration structures, and new research prospects in EMR and Data Security studies.

Table 2: Summary Characteristics of Reviewed Studies (n = 86)

Characteristic	Description
Publication period	2003–2025
Database source	Scopus
Document type	Peer-reviewed journal articles
Language	English
Dominant research domains	Health informatics, digital health, healthcare information systems, cybersecurity
Primary research focus	Electronic Medical Records (EMRs), data security, privacy protection
Leading contributing regions	Asia, Europe, North America
Major contributing countries	China, United States, India, Indonesia
Common methodological approaches	Conceptual analysis, system design studies, empirical case studies, mixed-methods research
Key technological themes	EMR systems, data security mechanisms, blockchain-based architectures, interoperability
Analytical techniques applied	Bibliometric mapping, keyword co-occurrence analysis, collaboration network analysis
Software tools used	VOSviewer

4. RESULTS

4.1 Publication Performance and Growth Trends

This section reports the publication performance and growth patterns of Electronic Medical Record (EMR) and Data Security research across 86 Scopus-indexed journal articles from 2003 to 2025.

The area of EMR and Data Security has been studied since 2003 and dominated until 2015. A clear trend in publication activity emerged after 2015, with a more pronounced surge after 2019. There were 13 articles published in 2025, the year with the highest number of publications, indicating that research output has continued throughout this period. Previous research works mainly considered record management and information retrieval, while some recent publications concentrate more on blockchain solutions, cloud-based encryption or artificial intelligence-driven data protection mechanisms (Han et al., 2025; Pokharel et al., 2025).

These publication trends provide an overview of the temporal development of EMR and Data Security research.

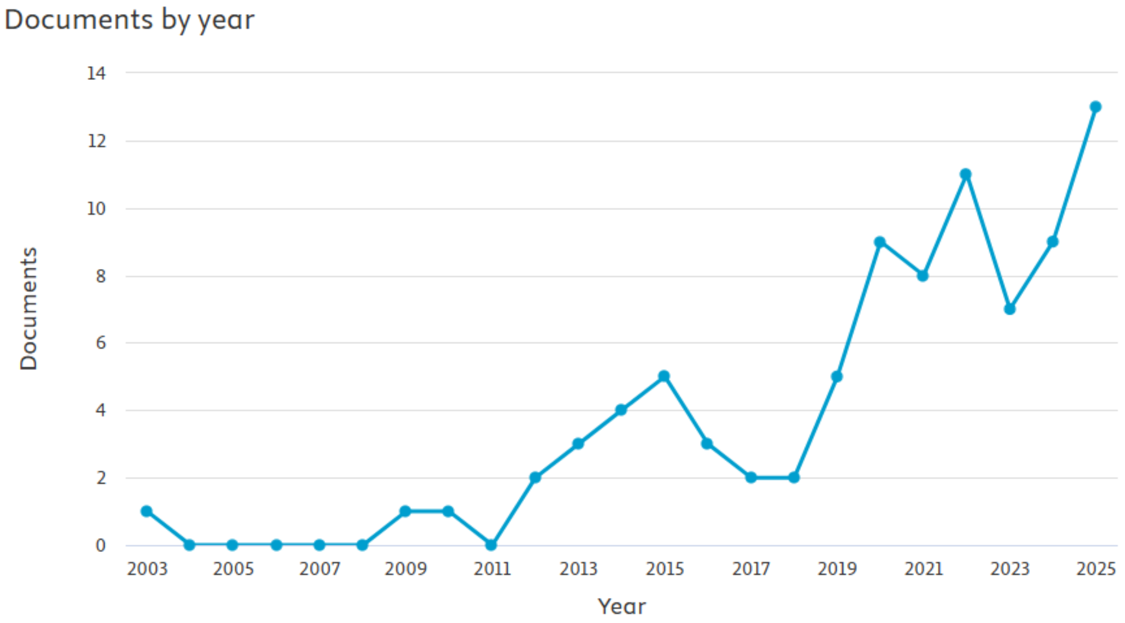

Figure 2: Annual number of publications on Electronic Medical Record and Data Security (2003–2025)

Source: Scopus database

4.2 Keyword Co-occurrence and Thematic Clusters

Keyword co-occurrence analysis revealed the predominant theme structures in the Electronic Medical Record (EMR) and Data Security literature. Using author keywords and bibliometric mapping, the study identifies three major underlying thematic clusters that describe the intellectual structure underpinning this area of enquiry.

The first group is mainly concerned with blockchain technology and encryption-protection schemes. Keywords in this cluster include blockchain, encryption, data integrity, and privacy, indicating research on the secure storage of medical records, protecting information from tampering, and providing limited access to EMR.

The second cluster is around the governance of digital health and interoperability protocols. Commonly appearing terms in this cluster are interoperability, data governance and privacy regulation, as well as health information systems, indicating works considering data management policies, regulatory compliance and cross-institutional exchange of healthcare-related data.

The third and growing class is represented by the smart healthcare and m-health applications. This cluster contains keywords such as Internet of Things (IoT), artificial intelligence, cloud computing, and mobile health (mHealth) which are studies combining state-of-the-art digital technologies to facilitate real-time data processing and EMR-based clinical services.

Net Overall, the key word analysis reveals a structured thematic pattern among technical security solutions, governance-oriented frameworks, and emerging smart healthcare applications within EMR and Data Security research.

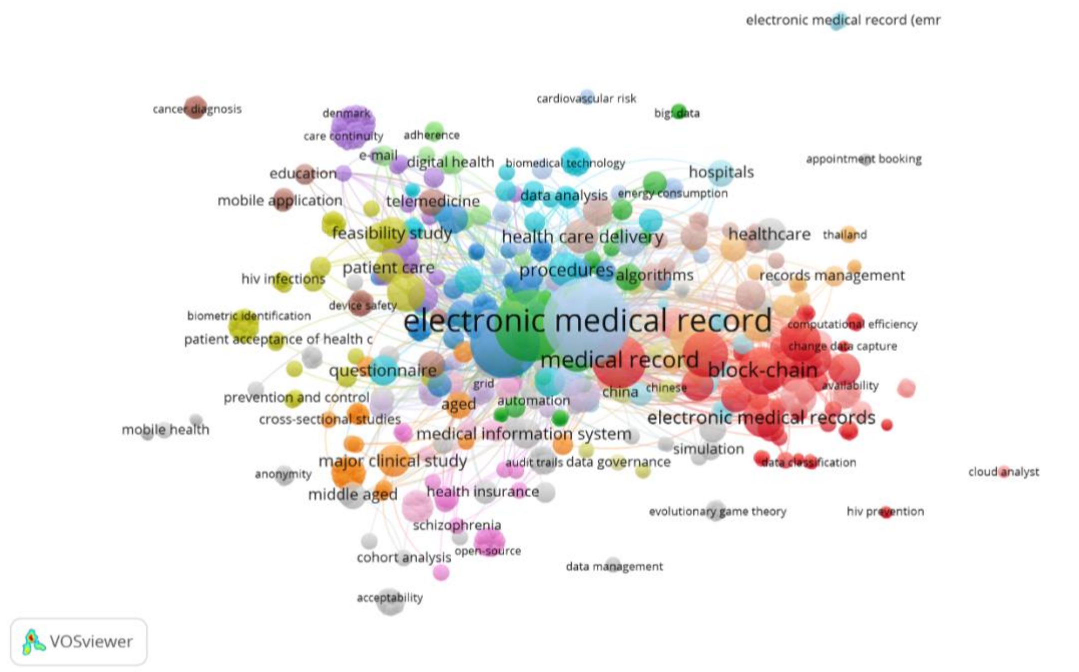

Figure 3: Keyword co-occurrence network of EMR and Data Security research
Source: Output VOSviewer software

Table 2: Keywords by authors

Rank	Keyword	Total link strength
1	Electronic medical record	1.404
2	Electronic health record	1.000
3	Electronic health records	961
4	Computer security	935
5	Medical record	552
6	Health care personnel	401
7	Data privacy	388
8	Block-chain	348
9	Data security	341

Source: Output VOSviewer software

4.3 Country-Level Contributions and International Collaboration

The bibliometric method illustrates that literature on the EMR and Data Security is spread over different countries and regions. According to the number of publications, China is the most productive country with over 20 papers, followed by the United States (18 papers), and India (10 papers). Other contributing countries are South Korea, United Kingdom, Australia, Indonesia and Ghana indicating a geographically diverse research environment.

The collaborations at international level are visualised in Figure 5, which offers a co-authorship networks among countries. The network also shows that the United States is a central hub for collaboration, with substantial collaborative links to China, the United Kingdom and Germany. Further collaboration links seen with India, South Korea and Australia indicating cross-regional involvement in EMR and Data Security research.

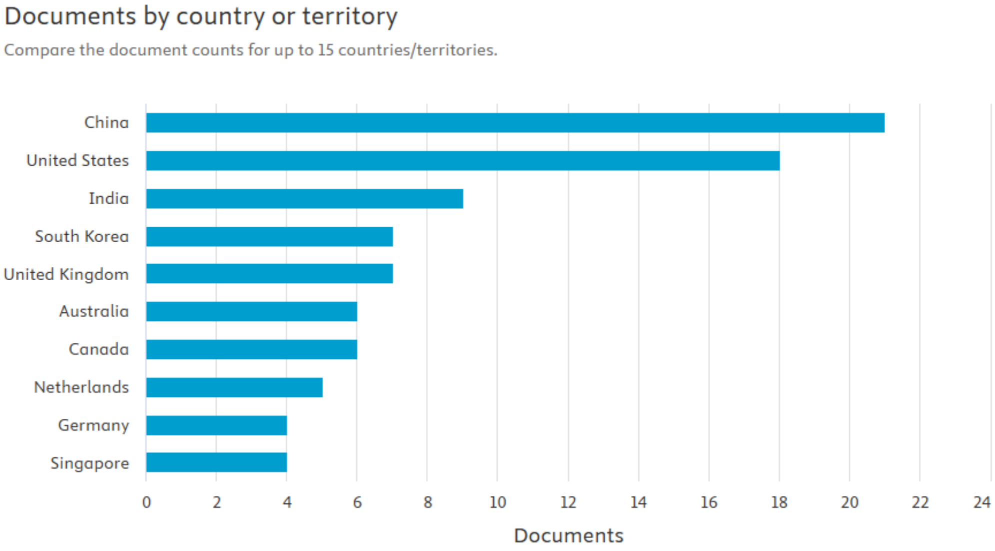

Figure 4: Distribution of publications by country

Source: Scopus database

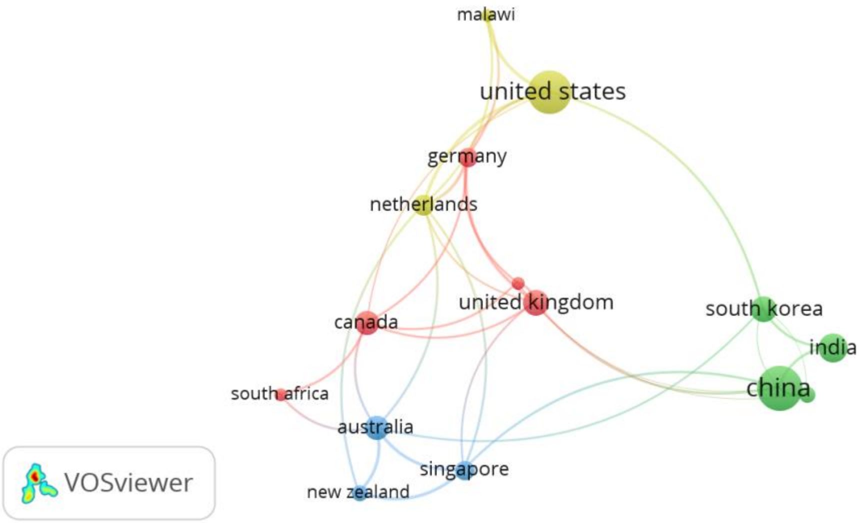

Figure 5: International collaboration network among countries

Source: Output VOSviewer software

4.4 Institutional Contributions

A cross-institution analysis demonstrates that EMR and the Data Security research is sponsored by a diverse set of academic, healthcare, and government institutions. University of the People's Republic of China is a major institution, followed by the King's College London and University of Washington, and Sichuan University as well which Rocked three papers. Other participating organizations are Massachusetts General Hospital, Harvard Medical School, Smart Healthcare Center of Excellence, the

Mayo Clinic, the University of Auckland and the University of Electronic Science and Technology of China.

The spectrum of institutional affiliations suggests representation from both developed and developing healthcare systems, and hails from across Asia, Europe, North America and Oceania.

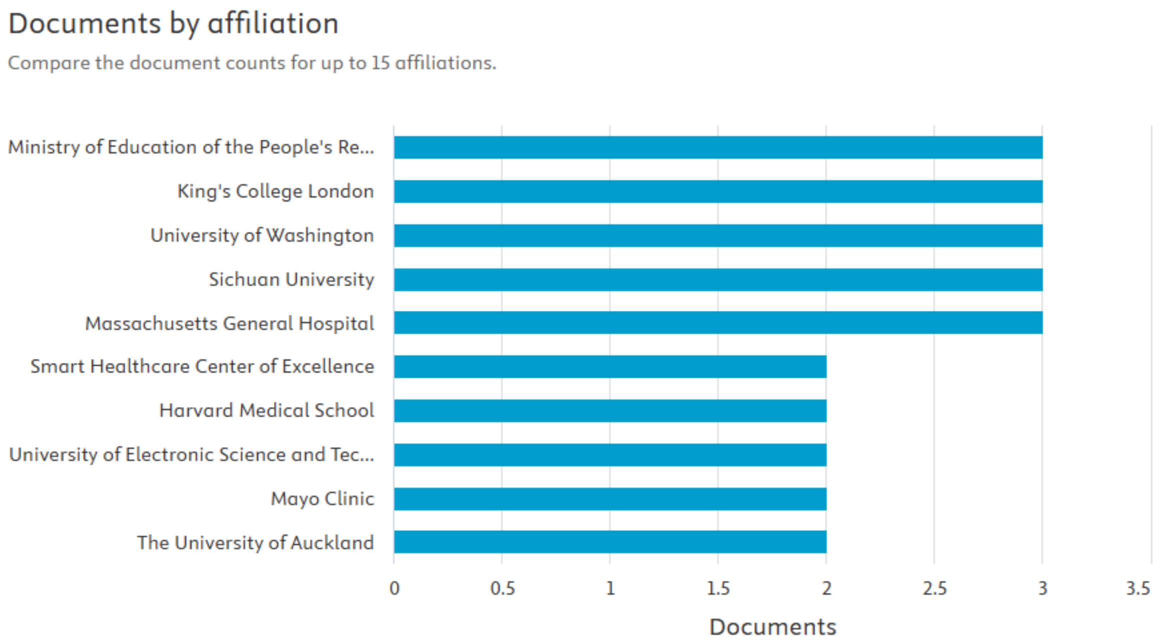

Figure 6: Top institutional affiliations contributing to EMR and Data Security research

Source: Scopus database

4.5 Journal Sources and Author Contributions

Analysis of journal sources demonstrates that the EMR and Data Security research output is distributed across a wide range of scientific outlets. Most publishing journals are IEEE Access, BMC Medical Informatics and Decision Making, and Journal of Medical Internet Research. These are the publications that most often publish on data encryption, blockchain security architecture, interoperable frameworks, and digital health information systems. There has been a gradual increase over time in the quantity of publication activity across journal sources until 2024, then a further increase in 2025.

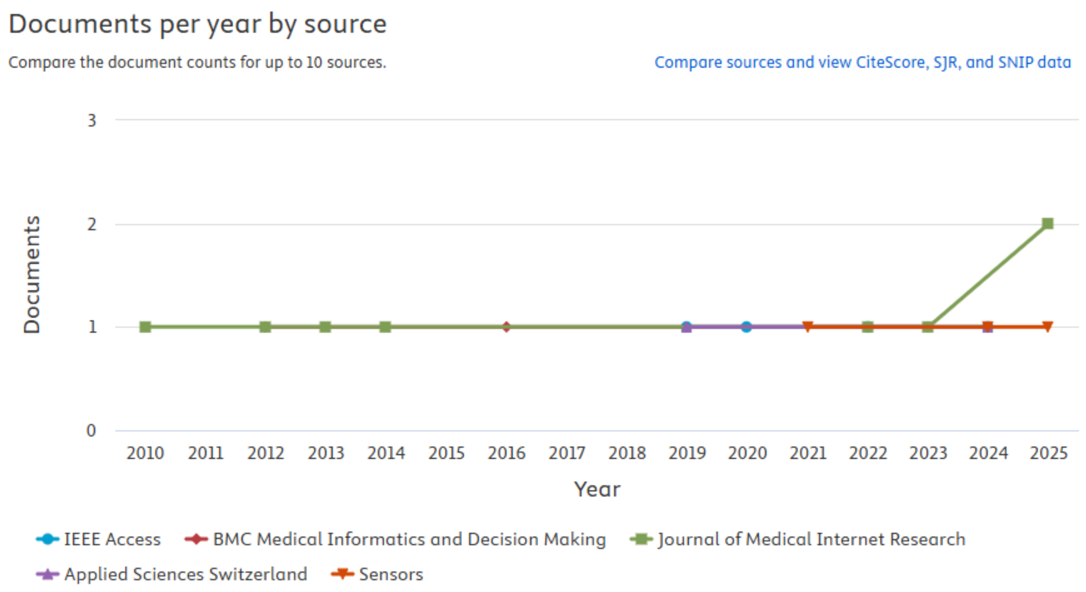

Figure 7: Number of articles by journal sources (top 10 journals)

Source: Scopus database

Author-level analysis: Author distribution in the EMR and Data Security research domain is quite scattered. No single author dominates publication output. The most active contributors, including Chiu, H.W., Hsu, C.Y., Kalra, D., Kim, D.H., Kung, H.H., Lee, H.A., Lee, Y.L., and Mars, M., each authored two publications. Additional authors, including Acheampong, P.R., and Agarwal, R., submitted a single article each.

The contributors serve as a multi-disciplinary research body covering health informatics, cyber security, medical systems, engineering, and the governance of digital health. This distribution of authorship demonstrates how engaging collaborative research is conducted across institutions and geographic locations.

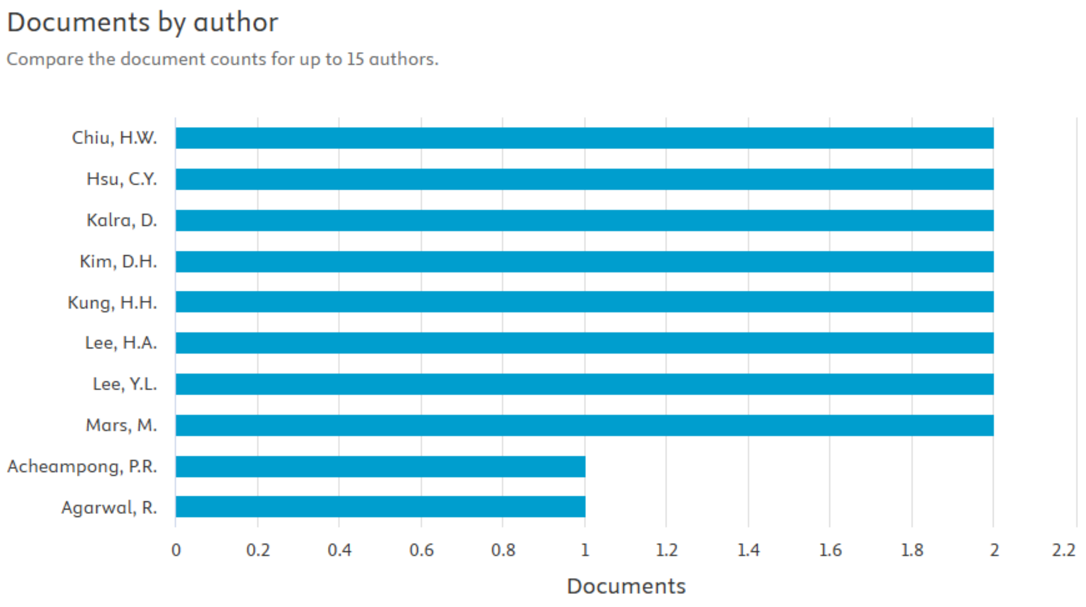

Figure 8: Top authors contributing to EMR and Data Security research

Source: Scopus database

5. DISCUSSION

5.1 Evolution of EMR and Data Security Research

The trends in research publications reflected in this work clearly demonstrate a significant boost in scholarly focus on EMR and Data Security research, particularly after 2015, with growth becoming exponential since 2019. This timing suggests an intersection of increased digital health expansion, greater recognition of cybersecurity threats to healthcare, and growing regulatory oversight in protecting patient data. Increasingly, however, rather than predominantly digitising information, recent research shows an emphasis on securing complex health information ecosystems in which processes are linked.

Evolution from early record-management studies to current research on blockchain, cloud security, and artificial intelligence indicates that the field has matured in exploring the systemic weaknesses and trust issues of eHealth systems. This evolution underscores that EMR data security has evolved from a technical support issue to an inherent part of the healthcare governance and risk paradigm.

5.2 Thematic Structure and Implications for Theory and Practice

The thematic groups derived from keyword co-occurrence analysis demonstrate that EMR and Data Security research are multifaceted, with multiple dimensions. Blockchains and encryption-based systems are becoming increasingly popular for decentralization and cryptography to improve data integrity and access control. Technical solutions alone don't cut it. Promotion of both governance and, to a lesser extent, interoperability research lines is also underpinned by the clear view that without societal systems able to support these technical changes, little real impact can be created (so technologies will remain stranded in their labs).

The development of smart healthcare and mobile health infrastructures is another example of how EMR systems are being integrated into real-time, data-rich care contexts. At a practical level, the identified themes highlight that healthcare organisations need to effectively balance technological innovations with readiness in governance, ensuring that data protection mechanisms are coherent with regulations, including at organisational levels, and that user confidence is maintained. This coexistence of the two clusters is relevant to researchers, underscoring the importance of integrative theoretical models that combine health informatics, cybersecurity, and information governance.

5.3 Geographic Distribution and Collaborative Dynamics

The national and institutional studies show that EMR and Data Security research is dispersed worldwide, contributed to by developed as well as developing health systems. International collaboration networks show growing cross-border research activity, especially among countries with digital health plans. These patterns of collaboration show that struggles related to EMR data security are not localized but rather global concerns, requiring collective knowledge-building.

The lack of a single leading author or institution also reflects the interdisciplinary and collaborative character of this research field. This diversity is a key element of methodological pluralism and extends the range of standpoints that can be taken regarding EMR security problems across varying healthcare settings and regulatory influences.

5.4 Theoretical Contributions and Future Research Agenda

This research offers a number of theoretical contributions to the EMR and Data Security literature. Firstly, the study extends a comprehensive mapping of worldwide knowledge structure by combining systematic literature review and bibliometric analysis, breaking through the confined fragmented technology-oriented or policy-designed analysis. This framework provides a longitudinal view of EMR security as an interdisciplinary research area at the intersection of health informatics, cybersecurity and healthcare governance.

Second, the discovery of three main thematic clusters provides a conceptual structure that helps understand the intellectual structure of EMR data security research. This work provides a theoretical integration of three perspectives on technology adoption, information governance and cybersecurity resilience.

Based on these findings, further studies can explore how new security technology interacts with governance sophistication, for example, in the areas of cross-border data flows and regulatory harmonization. More attention should also be given to human-centric factors, such as user trust, usability and behavioural reactions towards security mechanisms. Finally, generalizability will be improved, and theoretical development in the form of EMR data security research deepened if methodological approaches were extended by means of multi-database reviews and mixed methods research.

6. CONCLUSION

This paper synthesizes the global literature on Electronic Medical Records (EMRs) and data security by conducting an integrated systematic literature review and a bibliometric analysis of 86 articles from journals indexed in Scopus. The literature landscape, thematic structures, and collaborative relations were mapped to provide an integrated view of the development of EMR data security research in tandem with the digitalization and informatization of health care provision.

The results show that EMR information security has become a cross-disciplinary research area in the fields of technology application, data governance, and medical management. Instead of treating the security of EMR data as a purely technical problem, this has now been contextualized to encompass broader socio-technical issues such as interoperability, regulatory compliance, organizational readiness, and trust in digital health ecosystems. This change highlights the increasingly strategic role of data security in delivering accessible, high-quality and patient-centred healthcare.

More generally, this research adds to the literature by providing insights into the intellectual structure of EMR data security research and emphasizing the necessity of implementing an integrative and governance-based approach. Despite the considerable development that has taken place, there is still work to be done to increase the degree of conceptual integration and the methodological diversity in this territory. In conclusion, the study confirms that EMR data security will continue to be a cornerstone in building ethically operated, secure, and sustainable digital health systems globally.

REFERENCES

Carrera-Rivera, A., Ochoa, W., Larrinaga, F., & Lasa, G. (2022). How-to conduct a systematic literature review: A quick guide for computer science research. *MethodsX*, *9*, 101895. https://doi.org/10.1016/j.mex.2022.101895

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*(April), 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. T. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562. https://doi.org/10.1016/j.jbi.2012.12.003

Goldberg, D. G., Soylu, T. G., Hoffman, C. F., Kishton, R. E., & Cronholm, P. F. (2025). Clinicians' perspectives on the adoption and implementation of EMR-integrated clinical decision support tools in primary care. *Digital Health*, *11*. https://doi.org/10.1177/20552076251334043

Greenhalgh, T., Potts, H. W. W., Wong, G., Bark, P., & Swinglehurst, D. (2009). Tensions and paradoxes in electronic patient record research: A systematic literature review using the meta-narrative method. *Milbank Quarterly*, *87*(4), 729–788. https://doi.org/10.1111/j.1468-0009.2009.00578.x

Halid, M., & Binarto Budi Susilo, B. (2025). The role of field studying practices in improving understanding and skills for using electronic medical records among medical records and health information students. *Journal of Medical Education Development*, *18*(1), 87–95. https://doi.org/10.61186/edcj.18.1.87

Han, G., Ma, Y., Zhang, Z., & Wang, Y. (2025). A hybrid blockchain-based solution for secure sharing of electronic medical record data. *PeerJ Computer Science*, *11*. https://doi.org/10.7717/PEERJ-CS.2653

Kasim, Ö. (2022). An Efficient Ensemble Architecture for Privacy and Security of Electronic Medical Records. *International Arab Journal of Information Technology*, *19*(2), 272–280. https://doi.org/10.34028/iajit/19/2/14

Kim, M.-G., Hwang, G., Chang, J., Chang, S., Roh, H. W., & Park, R. W. (2025). Performance of Open-Source Large Language Models in Psychiatry: Usability Study Through Comparative Analysis of Non-English Records and English Translations. *Journal of Medical Internet Research*, *27*. https://doi.org/10.2196/69857

Liu, G., Xie, H., Wang, W., & Huang, H. (2024). A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. *Journal of Cloud Computing*, *13*(1). https://doi.org/10.1186/s13677-024-00608-w

Mishra, D. P., Rajeev, B., Mallick, S. R., Lenka, R. K., & Salkuti, S. R. (2025). Efficient blockchain based solution for secure medical record management. *International Journal of Informatics and Communication Technology*, *14*(1), 59–67. https://doi.org/10.11591/ijict.v14i1.pp59-67

Ndlovu, K., Mars, M., & Scott, R. E. (2021). Interoperability frameworks linking mHealth applications to electronic record systems. *BMC Health Services Research*, *21*(1). https://doi.org/10.1186/s12913-021-06473-6

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Systematic Reviews*, *10*(1), 1–11. https://doi.org/10.1186/s13643-021-01626-4

Papadopoulos, K., Ammenwerth, E., Lame, G., Stahl, N., Struckmann, V., von Wyl, V., & Gille, F. (2025). Understanding public trust in national electronic health record systems: A multi-national qualitative research study. *Digital Health*, *11*. https://doi.org/10.1177/20552076251333576

Pokharel, B. P., Kshetri, N., Sharma, S. R., & Paudel, S. (2025). blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems. *Information (Switzerland)*, *16*(2). https://doi.org/10.3390/info16020133

Pranckutė, R. (2021). Web of Science (WoS) and Scopus: the titans of bibliographic information in today's academic world. *Publications*, *9*(1). https://doi.org/10.3390/publications9010012

Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Information Management Journal*, *44*(3), 23–38. https://doi.org/10.1177/183335831504400304

Shahzad, A., Chen, W., Shaheen, M., Zhang, Y., & Ahmad, F. (2024). A robust algorithm for authenticated health data access via blockchain and cloud computing. *PLOS ONE*, *19*(9 September). https://doi.org/10.1371/journal.pone.0307039

Singh, Y., Jaiswal, S., & Kumar, V. (2024). A Comprehensive Literature Review on Privacy, Security, and Data Management in Healthcare. *2024 2nd International Conference on Disruptive Technologies, ICDT 2024*, 220–224. https://doi.org/10.1109/ICDT61202.2024.10489013

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*(August), 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Surasak, T. (2024). Blockchain-Enhanced Security and Efficiency for Thailand's Health Information System. *International Journal of Advanced Computer Science and Applications*, *15*(11), 1119–1125. https://doi.org/10.14569/IJACSA.2024.01511109

Tensen, P., Nikolajsen, M. B., Paul, S. K., Acheampong, P. R., Gaifém, F., Murunga Wekesah, F. M., Kirk, U. B., Owusu-Dabo, E., Kallestrup, P., Beune, E., Agyemang, C., & van de Vijver, S. (2025). Exploring Stakeholders' Perceptions of Electronic Personal Health Records for Mobile Populations Living in Disadvantaged Circumstances: A Multi-Country Feasibility Study in Denmark, Ghana, Kenya, and The Netherlands. *International Journal of Environmental Research and Public Health*, *22*(9). https://doi.org/10.3390/ijerph22091363

Wang, M., Li, S., Zheng, T., Li, N., Shi, Q., Zhuo, X., Ding, R., & Huang, Y. (2022). Big Data Health Care Platform With Multisource Heterogeneous Data Integration and Massive High-Dimensional Data Governance for Large Hospitals: Design, Development, and Application. *JMIR Medical Informatics*, *10*(4). https://doi.org/10.2196/36481

Yuan, B., & Li, J. (2019). The policy effect of the general data protection regulation (GDPR) on the digital public health sector in the european union: An empirical investigation. *International Journal of Environmental Research and Public Health*, *16*(6). https://doi.org/10.3390/ijerph16061070

Zhu, D., Li, Y., Zhou, Z., Zhao, Z., Kong, L., Wu, J., Zhao, J., & Zheng, J. (2025). Blockchain-Based Incentive Mechanism for Electronic Medical Record Sharing Platform: An Evolutionary Game Approach. *Sensors*, *25*(6). https://doi.org/10.3390/s25061904

Zhu, S., Xia, Y., Li, Q., & Chen, Y. (2025). Global geopolitical risk and financial stability: Evidence from China. *Finance Research Letters*, *72*(July 2024), 106501. https://doi.org/10.1016/j.frl.2024.106501