

Cybersecurity and Patient Data Protection in Healthcare: Research Trends and Organisational Challenges in the Context of NIS2

Rikardo Protrka

University North

Trg dr. Žarka Dolinara 1, Koprivnica, Croatia

rikardo.protrka@unin.hr

Antonija Srok

University of Rijeka, Faculty of Economics and Business

Department of Quantitative Economics

Ivana Filipovića 4, Rijeka, Croatia

antonija.srok@efri.uniri.hr

Abstract. Healthcare digitalisation has increased the use of patient data, but also created new cybersecurity risks. This paper examines recent research on healthcare cybersecurity and patient data protection in the context of NIS2, adopted in 2022 to strengthen cybersecurity obligations. We analysed 1,951 WoSCC articles published from 2023 to 2025 using bibliometric analysis, keyword co-occurrence and topic-trend analysis, and full-text content analysis of the ten most-cited articles. Article output increased, with security, blockchain, privacy, cybersecurity, and authentication central to the field. The findings suggest that secure digital healthcare also requires, in practice, organisational preparedness, interoperability, patient trust, governance, and implementation resources.

Keywords. digital health, electronic health records, interoperability, cybersecurity, NIS2 Directive, healthcare management

1 Introduction

The digitalisation of healthcare has made patient data more widely used, more connected, and more difficult to protect. Electronic health records (EHRs), telemedicine services, interoperable platforms, artificial intelligence (AI)-based tools, and connected medical devices can improve access to information and support more coordinated care. At the same time, they increase the number of systems, users, and data flows that need to be secured.

In healthcare, a cybersecurity incident is not simply a data-protection issue. It can also become an operational and clinical problem: electronic records may become unavailable, clinical workflows may be interrupted, treatment may be delayed, and patients' trust in digital services may weaken. Cybersecurity is therefore closely linked to patient safety and the

continuity of care. It also has an organisational dimension: healthcare providers need appropriate governance arrangements, technical safeguards, trained staff, and sufficient resources to manage risks effectively (Carello et al., 2023). The importance of these issues has increased following the adoption of the NIS2 Directive by the European Union in 2022 (European Commission, 2026). The Directive strengthens cybersecurity obligations for essential sectors, including healthcare, and places greater emphasis on risk management, organisational responsibility, and the resilience of information systems. Alongside the General Data Protection Regulation (GDPR) and other relevant regulatory frameworks, it highlights the need to protect sensitive patient data while maintaining the reliable operation of healthcare services (European Parliament and Council of the European Union, 2025).

Research on healthcare cybersecurity has expanded in recent years, but the literature remains spread across partly separate strands, including secure data sharing, EHRs, AI-based applications, connected devices, interoperability, and patient trust. Technical solutions remain important, but their practical value also depends on whether healthcare organisations have the governance, infrastructure, staff capacity, and resources needed to implement them safely (Lampropoulos et al., 2023). Given the breadth and rapid development of the field, bibliometric analysis is useful for identifying where research activity is concentrated and how topics are connected. It provides a systematic way to map the expanding body of research, identify publication and citation patterns, and examine how the main areas of interest are developing (Donthu et al., 2021). Bibliometric methods have been widely applied across scientific fields and, more recently, in digital-health research, where technological, clinical, organisational, and regulatory issues frequently overlap.

The purpose of this study is to map recent research on cybersecurity and information security in healthcare, with particular attention to the protection

and secure management of patient data. We analyse 1,951 articles from the Web of Science Core Collection (WoS CC) published between 2023 and 2025. We combine bibliometric performance analysis with keyword co-occurrence and topic-trend analyses, complemented by a full-text content analysis of the ten most-cited articles. This combined approach allows us to examine both the broader structure of the research field and the issues emphasised in its most influential articles. We describe the development of the field, identify its leading contributors and key research topics, and assess how closely the current literature relates to areas relevant to NIS2 implementation, including secure data governance, risk management, interoperability, organisational preparedness, and system resilience.

In doing so, the paper examines whether recent healthcare cybersecurity research reflects the practical conditions under which secure digital healthcare must be implemented. To address these aims, we answer the following research questions:

RQ1. How has research on cybersecurity and patient data protection in healthcare evolved from 2023 to 2025 in terms of scientific production?

RQ2. Which countries, affiliations, journals, authors, and articles are the most prominent contributors to this research field?

RQ3. Which author keywords, keyword co-occurrence patterns, and topic trends shape the current research landscape of cybersecurity and patient data protection in healthcare?

RQ4. Which technical, patient-related, organisational, and resource-related issues emerge from the most influential articles?

RQ5. How do the identified research themes relate to areas relevant to the implementation of the NIS2 Directive, particularly secure data governance, risk management, interoperability, organisational preparedness, and the resilience of healthcare information systems?

The remainder of the paper is organised as follows. Section 2 describes the data collection and preparation process. Section 3 presents the methodology used for the bibliometric and content analyses. Section 4 presents and discusses the results. Section 5 summarises the main conclusions, outlines the study limitations, and identifies directions for future research.

2 Data Collection

The data collection procedure followed established guidelines for bibliometric research (e.g., Donthu et al., 2021). We retrieved bibliographic records from the WoS CC, which is widely used in bibliometric studies because of its broad coverage of scientific journals and citation indexes (e.g., Pranckutė, 2021). We conducted a topic-based search covering article titles, abstracts,

and author keywords. The search was based on the following query:

*((NIS*2 directive) OR (network and information systems directive) OR (Directive 2022/2555) OR cybersecurit* OR (information securit*)) AND health* AND patient**

We retrieved the records on 8 June 2026 and restricted the search to English-language articles, review articles, and proceedings papers published between 2023 and 2025. The initial search yielded 1,986 articles. We imported the bibliographic records into R and assessed metadata completeness before conducting the analysis. Where possible, we used DOI-based lookup procedures to complete missing information. We also standardised cited references and merged duplicate citation variants, primarily on the basis of DOI information. After additional cleaning based on publication year, the final dataset included 1,951 articles published between 2023 and 2025. This final dataset formed the basis for the descriptive, bibliometric, and content analyses.

3 Methodology

We conducted the bibliometric analysis in R using the bibliometrix package and its Biblioshiny web interface (Aria & Cuccurullo, 2017). Following Donthu et al. (2021), the analysis combined performance analysis and science mapping.

The performance analysis examined annual scientific production, citation impact, document types, leading journals, authors, affiliations, countries, and patterns of international collaboration. At the journal level, we examined journal output and the concentration of articles across core journals using Bradford's Law. We also identified the ten most-cited articles and analysed their full texts qualitatively.

The science-mapping analysis focused on the conceptual structure of the field. We examined author-keyword frequencies and conducted a keyword co-occurrence analysis to identify relationships between research topics. We also analysed topic trends to examine how the focus of the literature developed during the observed period.

To complement the bibliometric analysis, we conducted a qualitative full-text content analysis of the ten most-cited articles. We identified recurring technical, patient-related, organisational, and resource-related issues and grouped them into four analytical categories. We then mapped these categories interpretatively to areas relevant to the implementation of the NIS2 Directive in healthcare, including secure data governance, risk management, interoperability, organisational preparedness, and the resilience of healthcare information systems.

4 Results and Discussion

4.1 Performance Analysis

The final dataset comprised 1,951 articles published between 2023 and 2025 across 931 sources. The average article age was 1.88 years, which reflects the intentionally recent publication window. The articles included 72,803 cited references and received an average of 7.92 citations per article. The dataset included 8,950 authors from 93 countries and 3,335 reported affiliations, with an average of 5.34 co-authors per article. International co-authorship accounted for 32.34% of the articles, showing that almost one-third of the articles involved cross-country collaboration. The dataset h-index was 50. Table 1 summarises the main characteristics of the dataset. For consistency, all records included in the analysis are referred to as articles throughout the paper, irrespective of their specific document type. The dataset consisted mainly of articles (1,461; 74.88%), followed by proceedings papers (253; 12.97%) and review articles (237; 12.15%).

Table 1. Main characteristics of the dataset

Indicator	Value
Publication period	2023–2025
Articles	1,951
Sources	931
Annual growth rate (%)	20.20
Average article age	1.88
Average citations per article	7.92
Cited references	72,803
Author keywords	5,884
Authors	8,950
Average co-authors per article	5.34
International co-authorship (%)	32.34
Dataset h-index	50
Number of countries	93
Number of affiliations	3,335

Fig. 1 visualises annual scientific production, while Table 2 presents the corresponding citation indicators. The number of articles rose from 508 in 2023 to 709 in 2024 and 734 in 2025. Most of this increase occurred between 2023 and 2024, when the number of articles grew by 39.6%. Growth continued in 2025, although at a slower rate of 3.5%. Overall, scientific production increased by 44.5% between 2023 and 2025, corresponding to an annual growth rate of 20.2%.

Articles published in 2023 had received an average of 13.46 citations per article by the time of data extraction, compared with 8.36 citations for articles published in 2024 and 3.65 for those published in 2025. This decline is expected because more recent articles

have had less time to accumulate citations. Using approximate citation windows adjusted to the extraction date, the mean annual citation rate declined from approximately 3.92 citations per article in 2023 to 3.44 in 2024 and 2.55 in 2025.

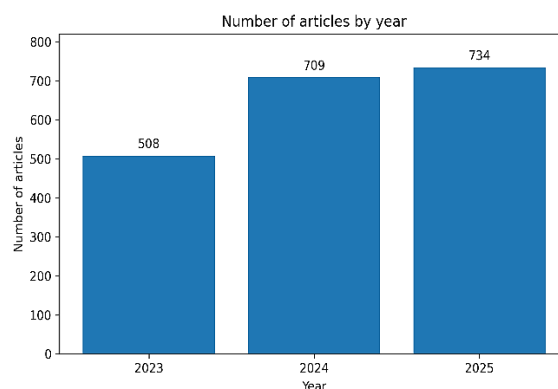


Figure 1. Annual scientific production

Table 2. Average citations by publication year

Year	Art. (n)	Cit. / art.	Cit. window (yrs)	Cit./art. /yr
2023	508	13.46	3.43	3.92
2024	709	8.36	2.43	3.44
2025	734	3.65	1.43	2.55

4.2 Leading countries, Affiliations, and Authors

Table 3 presents the leading countries based on the corresponding authors' affiliations. India accounted for the largest number of articles (367; 18.8%), followed by China (259; 13.3%) and the United States (227; 11.6%). Among the five most productive countries, the United Kingdom had the highest proportion of internationally co-authored articles (45.2%), followed by Saudi Arabia (40.6%) and China (29.0%). The broader geographical distribution of article production is shown in Fig. 2.

Table 3. Leading countries by corresponding author

Country	Art. (n)	Share (%)	International co-authorship (%)
India	367	18.8	20.2
China	259	13.3	29.0
United States	227	11.6	19.4
Saudi Arabia	96	4.9	40.6
United Kingdom	73	3.7	45.2

The leading affiliations and authors are summarised in Table 4. King Saud University was the most productive affiliation, with 42 articles, followed by

Sichuan University with 38 and the University of California San Diego with 36. At the author level, Zhang Y contributed the largest number of articles (17), followed by Wang Y (15) and Li J (12).

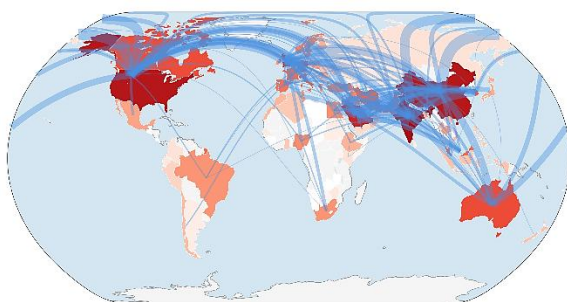


Figure 2. Geographical distribution of articles by corresponding author country

Table 4. Leading affiliations and authors

Affiliation	Art. (n)	Author	Art. (n)
King Saud University	42	Zhang Y.	17
Sichuan University	38	Wang Y.	15
University of California San Diego	36	Li J.	12
Princess Nourah bint Abdulrahman University	32	Kumar K.	11
University of Pennsylvania	31	Wang H.	10

4.3 Influential Journals

The articles were distributed across a large number of journals, indicating that research on cybersecurity and patient data protection in healthcare spans both technical and health-related fields. As shown in Table 5, IEEE Access was the most productive journal, with 51 articles, followed by the Journal of Medical Internet Research with 49 articles and Scientific Reports with 39 articles. Other prominent journals included the IEEE Internet of Things Journal, Sensors, and Electronics. Fig. 3 presents the development of article output among the leading journals during the observed period.

Table 5. Most productive journals

Journal	Art. (n)
IEEE Access	51
Journal of Medical Internet Research	49
Scientific Reports	39

Journal	Art. (n)
IEEE Internet of Things Journal	28
Sensors	27
Electronics	25
International Journal of Advanced Computer Science and Applications	24
Applied Sciences	22
Cureus Journal of Medical Science	22
BMC Health Services Research	21

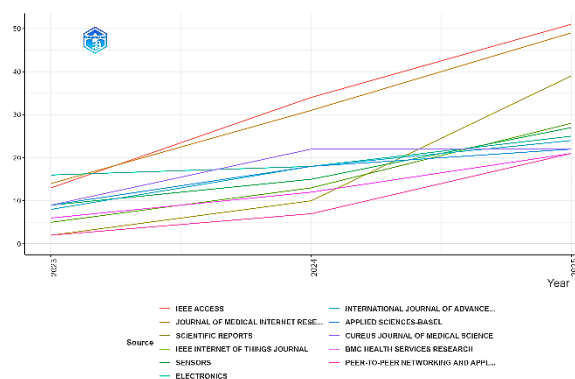


Figure 3. Production of the leading journals over time

Even the most productive journal accounted for only 2.6% of all articles, confirming that the literature is relatively dispersed. However, Bradford's Law identified a smaller group of 38 core journals, representing 4.1% of all sources, which published approximately one-third of the articles. Beyond this core group, the remaining articles were distributed across a much larger number of journals.

4.4 Keyword Analysis and Topic Trends

The most frequent author keywords are presented in Table 6, while Fig. 4 shows their co-occurrence network. Security was the most frequently used keyword, appearing 396 times, followed by blockchain (293), privacy (278), healthcare (236), and cybersecurity (166). Other prominent keywords included internet, artificial intelligence, health, care, and authentication. These results place security, privacy, blockchain, cybersecurity, and authentication at the centre of the field, while broader terms such as healthcare, health, and care reflect the search scope and clinical context.

Table 6. Most frequent author keywords

Keyword	Freq.
Security	396
Blockchain	293
Privacy	278

Keyword	Freq.
Healthcare	236
Cybersecurity	166
Internet	163
Artificial intelligence	142
Health	123
Care	122
Authentication	103

The keyword co-occurrence network reveals several closely connected thematic areas. Security, privacy, blockchain, and authentication form a central group of concepts, while artificial intelligence and related data-driven technologies appear as an increasingly important strand of research.

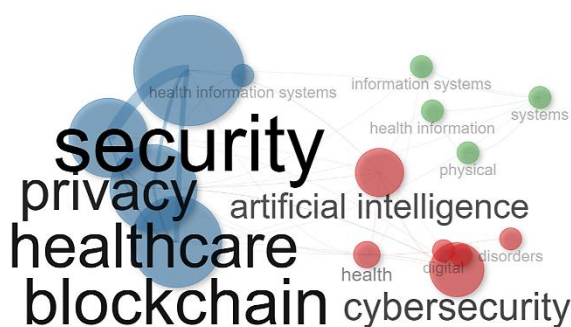


Figure 4. Keyword co-occurrence network

Fig. 5 presents the temporal development of the main trend topics. Security, blockchain, and privacy remained prominent throughout the observed period. AI-related terms became more visible in the later part of the period, with median year of occurrence being 2025. By contrast, COVID-19, mobile health, and privacy protection were more strongly associated with the earlier part of the analysed period. The results suggest a shift from broader digital-health and privacy concerns towards AI-related security challenges and privacy-preserving approaches.

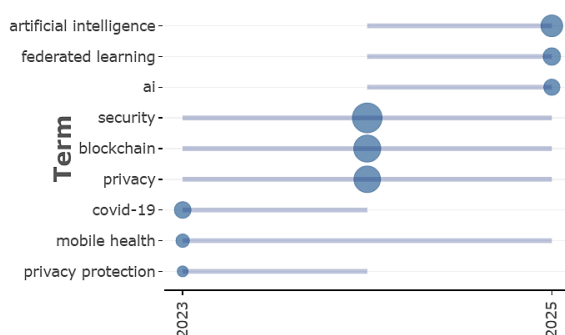


Figure 5. Trend topics in cybersecurity and patient data protection research

4.5 Content Analysis of the Most-Cited Articles

To identify the main practical issues raised in the most-cited literature, we conducted a qualitative full-text content analysis of the ten most-cited articles in the dataset. As shown in Table 7, these articles had received between 119 and 289 citations in the Web of Science Core Collection by the date of data extraction. The selected articles address a diverse range of technologies and implementation settings. AI-related issues are particularly prominent, including privacy-preserving AI, generative AI, large language models (LLMs), and AI-enabled wearable sensors. Other articles focus on metaverse healthcare, internet of medical things (IoMT) vulnerabilities, medical-image encryption, and the adoption of personal health records.

Table 7. Most-cited articles included in the content analysis

Author (yr)	Main focus	Cit.
Khalid et al. (2023)	Privacy-preserving AI and secure health-data use	289
Chengoden et al. (2023)	Metaverse healthcare, interoperability, privacy, and cost	230
Eggmann et al. (2023)	LLM use in dental medicine, reliability, and cybersecurity	204
Paul et al. (2023)	Digital healthcare, IoMT vulnerabilities, and cyber-risk controls	172
Chen and Esmaeilzadeh (2024)	Generative-AI risks across the system life cycle	170
Wu et al. (2023)	Secure transmission and encryption of medical images	168
Jeyaraman et al. (2023)	AI ethics, accountability, transparency, and data stewardship	166
Chen et al. (2025)	Wearable sensors, AI integration, reliability, and infrastructure constraints	124
Wang and Zhang (2024)	LLM applications, data security, hallucinations, bias, and accountability	122
Alsyounf et al. (2023)	Patient adoption of personal health records: privacy, security, and usability	119

Despite their different areas of focus, the selected articles identify several recurring concerns. The most prominent issues relate to the secure use and management of patient data and the growing complexity of digital healthcare systems. The articles identify vulnerabilities affecting EHRs, personal health

records, AI applications, connected devices, wearable sensors, and emerging virtual-care environments. Although these technologies may improve access, monitoring, and clinical decision support, their safe implementation depends on reliable data, privacy protection, secure data transmission, interoperability, appropriate organisational controls, and sufficient technical and human resources. Based on the full-text analysis, we grouped the identified issues into four analytical categories: technical, patient-related, organisational, and resource-related issues. Table 8 summarises the main issues within each category.

Table 8. Main issues identified in the selected articles

Category	Main issues
Technical issues	Protection of sensitive health data; cyberattacks affecting EHRs, connected devices, AI systems, and data transmission; fragmented and non-standardised data; limited interoperability; inaccurate or biased AI outputs; insufficient explainability
Patient-related issues	Privacy and confidentiality concerns; trust in digital systems; usability and ease of use; risk of misinformation; unequal access to digital services; reduced personal interaction
Organisational issues	Unclear accountability; limited governance frameworks; weak cybersecurity preparedness; insufficient monitoring and validation; poor integration into clinical workflows; need for staff training and human oversight
Resource-related issues	High implementation and infrastructure costs; limited curated datasets; computational requirements; battery and energy constraints in wearable devices; affordability and workforce capacity

The content analysis therefore shifts the interpretation from cybersecurity as a technical problem to cybersecurity as an implementation and governance problem. Secure data governance, structured risk management, interoperable infrastructures, clear organisational responsibilities, and resilience under cyberattack or system failure are closely interconnected. Patient trust and system usability are also relevant because secure digital services need to be accepted and used appropriately.

We then mapped these categories interpretatively to areas relevant to the implementation of the NIS2 Directive, including secure data governance, risk management, interoperability, organisational preparedness, and the resilience of healthcare

information systems, as shown in Table 9. The mapping is interpretative rather than direct because most of the selected articles do not explicitly examine the NIS2 Directive or assess compliance with its requirements. Nevertheless, their findings provide a practical rationale for the Directive's emphasis on risk management, organisational preparedness, and resilience.

Table 9. Relevance of the identified issues to areas associated with NIS2 implementation

Category	NIS2 relevance
Technical issues	Secure data governance; risk management; interoperability; system resilience
Patient-related issues	Secure data governance; risk management; organisational preparedness
Organisational issues	Organisational preparedness; risk management; interoperability
Resource-related issues	System resilience; organisational preparedness; risk management

5 Conclusion

This study examined recent research on cybersecurity and information security in healthcare, with particular attention to the protection and secure management of patient data. Based on 1,951 articles published between 2023 and 2025, the findings show that the field is expanding rapidly but remains distributed across several technical and health-related domains. Scientific production increased during the observed period, while the dispersion of articles across many journals reflects the interdisciplinary nature of the topic. The keyword analysis shows that security, blockchain, privacy, cybersecurity, and authentication remain central areas of interest. The emergence of artificial intelligence and federated learning points to new challenges associated with the secure use of increasingly data-intensive technologies. These developments are particularly relevant in healthcare, where digital innovation depends on the availability, quality, and secure exchange of sensitive patient data.

The full-text content analysis of the ten most-cited articles identified four closely connected categories of issues: technical, patient-related, organisational, and resource-related. Although technical safeguards remain essential, their effective implementation also depends on reliable data governance, interoperable and resilient information systems, clear organisational responsibilities, patient trust, and adequate resources. The identified issues are closely related to areas relevant to the implementation of the NIS2 Directive in healthcare, particularly risk management, organisational preparedness, and system resilience.

However, this relationship is interpretative rather than direct, as most articles do not explicitly examine the Directive or assess compliance with its requirements.

This study has several limitations. The analysis was restricted to English-language articles indexed in the Web of Science Core Collection and published between 2023 and 2025. Citation indicators should be interpreted cautiously because more recent articles have had less time to accumulate citations. The content analysis was also limited to the ten most-cited articles, while the mapping to areas relevant to NIS2 implementation reflects an analytical interpretation rather than a regulatory assessment. Future research should examine the implementation of cybersecurity measures in real healthcare settings, with particular attention to organisational readiness, interoperability, resource constraints, the economic implications of cybersecurity investment, and the safe integration of AI-based tools into clinical workflows. As healthcare systems become increasingly dependent on digital infrastructure, cybersecurity should be treated as an integral component of patient safety, organisational resilience, and sustainable healthcare management.

References

- Alsyouf, A., Lutfi, A., Alsubahi, N., Alhazmi, F. N., Al-Mugheed, K., Anshasi, R. J., Alharbi, N. I., & Albugami, M. (2023). The use of a technology acceptance model (TAM) to predict patients' usage of a personal health record system: The role of security, privacy, and usability. *International Journal of Environmental Research and Public Health*, 20(2), 1347. <https://doi.org/10.3390/ijerph20021347>
- Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, 11(4), 959–975. <https://doi.org/10.1016/j.joi.2017.08.007>
- Carello, M. P., Marchetti Spaccamela, A., Querzoni, L., & Angelini, M. (2023). A systematization of cybersecurity regulations, standards and guidelines for the healthcare sector. *arXiv*. <https://arxiv.org/abs/2304.14955>
- Chen, S., Fan, S., Qiao, Z., Wu, Z., Lin, B., Li, Z., Riegler, M. A., Wong, M. Y. H., Opheim, A., Korostynska, O., Nielsen, K. M., Glott, T., Martinsen, A. C. T., Telle-Hansen, V. H., & Lim, C. T. (2025). Transforming healthcare: Intelligent wearable sensors empowered by smart materials and artificial intelligence. *Advanced Materials*, 37, 2500412. <https://doi.org/10.1002/adma.202500412>
- Chen, Y., & Esmaeilzadeh, P. (2024). Generative AI in medical practice: In-depth exploration of privacy and security challenges. *Journal of Medical Internet Research*, 26, e53008. <https://doi.org/10.2196/53008>
- Chengoden, R., Victor, N., Huynh-The, T., Yenduri, G., Jhaveri, R. H., Alazab, M., Bhattacharya, S., Hegde, P., Maddikunta, P. K. R., & Gadekallu, T. R. (2023). Metaverse for healthcare: A survey on potential applications, challenges and future directions. *IEEE Access*, 11, 12765–12795. <https://doi.org/10.1109/ACCESS.2023.3241628>
- 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, 285–296. <https://doi.org/10.1016/j.jbusres.2021.04.070>
- Eggmann, F., Weiger, R., Zitzmann, N. U., & Blatz, M. B. (2023). Implications of large language models such as ChatGPT for dental medicine. *Journal of Esthetic and Restorative Dentistry*, 35(7), 1098–1102. <https://doi.org/10.1111/jerd.13046>
- European Commission. (2026). NIS2 Directive: Securing network and information systems. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
- European Parliament and Council of the European Union. (2025). Regulation (EU) 2025/327 on the European Health Data Space. *Official Journal of the European Union*, L 2025/327. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R0327>
- Jeyaraman, M., Balaji, S., Jeyaraman, N., & Yadav, S. (2023). Unraveling the ethical enigma: Artificial intelligence in healthcare. *Cureus*, 15(8), e43262. <https://doi.org/10.7759/cureus.43262>
- Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in Biology and Medicine*, 158, 106848. <https://doi.org/10.1016/j.compbiomed.2023.106848>
- Lampropoulos, K., Zarras, A., Lakka, E., Barmdaki, P., Drakonakis, K., Athanatos, M., Debar, H., Alexopoulos, A., Sotiropoulos, A., Tsakirakis, G., Dimakopoulos, N., Tsolovos, D., Pocs, M., Smyrlis, M., Basdekis, I., Spanoudakis, G., Mihaila, O., Prelipcean, B., Salant, E., ... Khabbaz, M. D. (2023). White paper on cybersecurity in the healthcare sector: The HEIR solution. *arXiv*. <https://arxiv.org/abs/2310.10139>
- Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, 9, 571–588. <https://doi.org/10.1016/j.icte.2023.02.007>
- Pranckutė, R. (2021). Web of Science (WoS) and Scopus: The titans of bibliographic information in

today's academic world. *Publications*, 9(1), 12.
<https://doi.org/10.3390/publications9010012>

Wang, D., & Zhang, S. (2024). Large language models in medical and healthcare fields: Applications, advances, and challenges. *Artificial Intelligence Review*, 57, Article 299.
<https://doi.org/10.1007/s10462-024-10921-0>

Wu, Y., Zhang, L., Berretti, S., & Wan, S. (2023). Medical image encryption by content-aware DNA computing for secure healthcare. *IEEE Transactions on Industrial Informatics*.
<https://doi.org/10.1109/TII.2022.3194590>