GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v3i2.

The Urgency of Legal Protection for Electronic Medical Records Amid Cybercrime Threats: A Literature Review on Patients' Rights and Doctors' Obligations

Ade Netra Kartika[1]
[1]Universitas Borobudur, Jakarta, Indonesia, ade_netra@yahoo.com

Corresponding Author: ade_netra@yahoo.com[1]

Abstract: The digitization of electronic medical records (EMRs) has revolutionized healthcare delivery globally. However, alongside efficiency and accessibility, EMRs pose increasing risks due to cybercrime. Sensitive health data is now vulnerable to unauthorized access, requiring not only technological safeguards but also a strong legal framework. This literature review aims to map existing academic discussions and research findings on the legal protection of EMRs, with a focus on patients' rights to privacy and the legal obligations of healthcare providers. Through a systematic analysis of international and Indonesian literature published over the last five years, this study identifies trends, regulatory gaps, and conceptual frameworks that inform the evolving intersection of law, technology, and health data governance. The findings reveal fragmented regulatory responses and a need for integrative legal models to address cyber threats in the health sector. Recommendations include cross-disciplinary legal reform, improved cybersecurity standards, and enhanced legal literacy for medical professionals.

Keywords: Electronic Medical Records, Cybercrime, Legal Protection, Privacy Rights, Healthcare Law, Literature Review

INTRODUCTION

The digital revolution in healthcare is reshaping how medical information is collected, stored, accessed, and utilized M. Zimoń and R. Kasprzyk. (2021) D. Dhingra and A. Dabas. (2020). V. Popa et al., (2024). Among the most transformative tools in this transition is the Electronic Medical Record (EMR) N. Amalia, M. Z. Azhri, A. Rosarini, D. R. Wijayanti, and M. A. Riestiyowati, (2021), which enables seamless, real-time, and longitudinal tracking of patient data. The adoption of EMRs has brought numerous benefits, such as improved coordination of care, enhanced diagnostic accuracy, streamlined workflows, and better patient outcomes. By facilitating interoperability between healthcare providers, EMRs are also playing a pivotal role in promoting integrated health systems and data-driven public health strategies.

However, alongside these benefits lie serious risks. The increasing digitization of sensitive health information has made healthcare systems attractive targets for malicious cyber actors. In recent years, the frequency and severity of cybercrime incidents in the health sector have escalated at an alarming rate A. Rollins. (2016) S. Monteith, T. Glenn, J. R. Geddes. (2024). C. Santos. (2020). Hospitals and medical institutions have become primary targets for ransomware attacks, data theft, phishing scams, and unauthorized access to medical records J. Li and M. J. Shaw. (2012).

Indonesia has not been immune to this trend Y. K. WINDI. (2018). Several cases of data breaches involving healthcare institutions and national health systems have highlighted the country's inadequate preparedness to face growing cybercrime threats A. Wirth. (2011). Weak digital infrastructure, limited cybersecurity protocols, and fragmented legal protections contribute to the vulnerability of electronic health information. These incidents underscore the urgent need for stronger legal frameworks to ensure the security, confidentiality, and integrity of EMRs.

This situation reveals a critical phenomenon gap. While technological innovation in healthcare is progressing rapidly, the legal and regulatory environment has not evolved at the same pace. The rise of cybercrime has exposed serious shortcomings in existing laws and institutional capacities, particularly with respect to data protection, breach notification, and the accountability of service providers A. Rollins. (2016) S. Monteith, T. Glenn, J. R. Geddes. (2024), A. Wirth. (2011). S. Ghosh and E. Turrini. (2010). R. G. Smith. (2015). Legal instruments tailored to the specific needs of the digital health ecosystem -particularly those governing EMRs- are often absent or inconsistently implemented.

Parallel to the phenomenon gap, a clear research gap also emerges. Although cybercrime in the healthcare sector has become a growing concern S. Monteith, T. Glenn, J. R. Geddes. (2024). C. Santos. (2020) Hassan Samkari and Adnan Gutub, (2015), most academic studies on EMRs tend to focus on technical design, data management efficiency, or clinical outcomes. There is relatively little research examining the legal and ethical dimensions of EMRs, especially in the context of data security, patient consent, and the liability of healthcare professionals and institutions. The interdisciplinary nature of these challenges—where law intersects with information systems, ethics, and public health—demands scholarly attention that bridges these domains.

This leads to the central research problem of this review: How does existing academic literature address the adequacy and limitations of legal protection for EMRs, particularly in safeguarding patient privacy and clarifying the responsibilities of healthcare professionals amid growing cybercrime threats?

The purpose of this study is to conduct a structured literature review that maps and synthesizes academic discourse on the legal dimensions of EMRs. This includes examining legal frameworks, identifying thematic concerns such as privacy rights and informed consent, evaluating the responsibilities of healthcare actors, and highlighting policy recommendations that can help address vulnerabilities in the current system.

The novelty of this article lies in its integrative and analytical approach. Unlike normative legal discussions that typically center on specific doctrines or case law, this review draws on a wide range of interdisciplinary sources to explore how legal scholarship is responding to the challenges of cybercrime in healthcare. By doing so, it offers a broader understanding of the evolving legal landscape surrounding EMRs, particularly within the Indonesian context, and contributes to the global conversation on digital health governance. The study also provides actionable insights for legal scholars, policymakers, and health practitioners seeking to strengthen legal infrastructure and data protection mechanisms in the age of digital medicine.

LITERATURE REVIEW

This section presents a synthesis of existing literature thematically grouped into four key domains. First, legal and regulatory frameworks for EMRs. Second, patients' privacy rights and ethical concerns. Third, healthcare providers' legal responsibilities, and last, cybercrime risks and systemic vulnerabilities in digital healthcare.

Legal and Regulatory Frameworks

Scholars widely acknowledge that legal and regulatory frameworks governing EMRs remain underdeveloped in many countries, particularly in low- and middle-income nations. Several studiesc M. K. Hossain, J. Sutanto, P. W. Handayani, A. A. Haryanto, J. Bhowmik, and V. Frings-Hessami. (2025). C. George and B. Berčič. (2009), (e.g., Hossain et al., 2025; Nurhayati et al., 2024) stress that current legal mechanisms lack clarity regarding data ownership, cross-border data transfer, and sector-specific cybersecurity obligations. In Indonesia, the Personal Data Protection Law (UU PDP 2022) introduces general data protection principles but does not elaborate on obligations tailored to healthcare settings .

Comparative literature highlights the importance of sector-specific instruments such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States J. N. Weiss. (2023) and the General Data Protection Regulation (GDPR) in the European Union B. Yuan and J. Li. (2019). These laws are praised for their enforcement mechanisms, defined data controller responsibilities, and provisions for data breach notification.

Scholars argue that Indonesia could benefit from adapting similar principles, particularly by specifying roles for hospitals and healthcare professionals as data controllers or processors under domestic law N. Amalia, M. Z. Azhri, A. Rosarini, D. R. Wijayanti, and M. A. Riestiyowati, (2021) M. K. Hossain, J. Sutanto, P. W. Handayani, A. A. Haryanto, J. Bhowmik, and V. Frings-Hessami. (2025). M. Sumarto and A. Kaasch, (2018). A. Booth, R. M. Purnagunawan (2019).

Studies also suggest the need for integrated regulatory approaches that combine health law, information technology law, and consumer protection C. George and B. Berčič (2009), P. S. C. MZ and R. Sidi. (2025), V. Janarthanan, N. V Nagrale, O. G. Singh, K. V Raj. (2024). This integration is necessary because EMRs do not merely represent a medical issue but rather intersect with digital identity, security governance, and public trust.

Patients' Privacy Rights and Ethical Concerns

Privacy emerges as one of the most discussed issues in the literature on EMRs. Researchers assert that EMRs carry the potential to infringe on patient autonomy when not governed by explicit consent and access protocols S. Thakral and A. Vaish. (2022). Informed consent is no longer a one-time agreement; in digital systems, it must be continuous and granular—allowing patients to understand, restrict, or withdraw access to their data.

Ethical concerns also surface regarding the secondary use of EMRs for research, insurance, or commercial purposes P. S. C. MZ and R. Sidi. (2025). V. Janarthanan, N. V Nagrale, O. G. Singh, K. V Raj. (2024). S. John, N. Ravichandran, and M. F. Khan. (2018). Some scholars criticize vague regulations that allow data anonymization as a loophole to bypass consent requirements. Others raise concerns about inequality in digital literacy, which may disproportionately impact marginalized groups who are less able to navigate consent mechanisms or comprehend privacy notices.

In this context, literature calls for legal empowerment strategies, where patients are not only informed about their rights but also supported through accessible grievance mechanisms. Regulatory frameworks must balance innovation and efficiency with the ethical imperatives of autonomy, non-maleficence, and justice.

Legal Responsibilities of Healthcare Providers

EMR protection is not only about system security, it also depends on the legal duties of those who manage, process, and access medical data. Studies emphasize the lack of specific statutory obligations for doctors and hospital management teams to implement cybersecurity protocols J. Villalobos and N. Calvanese. (2021). Legal liability for data breaches is often unclear, especially when breaches occur due to third-party service providers or infrastructure weaknesses.

In jurisdictions governed by GDPR or HIPAA, healthcare professionals are obligated to conduct impact assessments, maintain audit trails, and report security incidents. These measures help ensure accountability. However, in many countries -including Indonesia- regulatory ambiguity allows institutions to shift responsibility between IT vendors, hospital administrators, and individual practitioners.

Academic discussions highlight the concept of "digital negligence" F. Pazarcıkcı, N. Karataş, and A. Kaya (2024) as an emerging area of tort law, where failure to implement standard cybersecurity measures could constitute professional misconduct or legal breach. This growing body of literature calls for legal doctrines that define duty of care in digital health settings.

Cybercrime and Vulnerabilities in the Healthcare Sector

The literature is increasingly recognizing cybercrime as one of the most critical threats to EMR systems S. Xu, J. Ning, Y. Li, Y. Zhang, G. Xu, (2021). Healthcare is now considered the second-most targeted sector for cybercrime, following finance. Multiple studies document cases of ransomware attacks that disabled hospital operations, exfiltrated health data, and extorted healthcare institutions. In Indonesia, systemic issues such as outdated software, lack of endpoint protection, and insufficient training make hospitals susceptible to infiltration.

Researchers argue that existing laws are ill-equipped to address complex cybercrime scenarios M. S. Anker, S. Hadzibegovic, A. Lena, and W. Haverkamp. (2019). For example, the Electronic Information and Transactions Law (ITE) in Indonesia outlines general penalties for data misuse but does not establish technical standards for breach prevention or institutional accountability. This leads to a reactive rather than preventive legal culture.

METHOD

This study adopts a systematic literature review (SLR) methodology to examine how academic literature addresses the legal protection of electronic medical records (EMRs) in response to rising cybercrime threats. The review integrates both Scopus-indexed sources and broader academic discourse captured through Google Scholar.

This review incorporates two key academic databases to ensure both depth and breadth in coverage. The Scopus database was chosen for its high-quality, peer-reviewed, and indexed sources that ensure academic rigor and international relevance R. Pranckutė (2021), Budiman (2023). However, given the narrow results retrieved from Scopus—yielding only three specific conference papers focused on EMR cybersecurity—Google Scholar was also utilized to broaden the search scope.

Google Scholar was selected due to its inclusivity and ability to capture grey literature, policy discussions, and emerging interdisciplinary work that may not yet be indexed in Scopus R. Pranckutė (2021). The citation-based selection ensures that the review includes articles recognized as influential or foundational in the evolving discourse on EMRs and cybercrime. The initial search was conducted using Publish or Perish software, filtered through the Scopus database, yielding three relevant studies focused on cybersecurity measures in EMRs. To broaden the scope, an extended search was performed using Google Scholar, which returned over 200 potentially relevant documents. From these, the top 15 most cited articles were selected for in-depth analysis, based on citation count, relevance to legal and cybersecurity issues in EMRs, and their publication between 2018 and 2025**.**

Articles were included if they addressed the intersection of EMRs and cybersecurity or cybercrime; contained legal, ethical, or policy analysis; were written in English or Bahasa Indonesia and were peer-reviewed journal articles, conference papers, or legal commentaries.

A thematic content analysis was used to categorize and synthesize the literature. Each selected article was coded manually, and themes were developed inductively based on recurring topics across texts. Four dominant themes emerged and were used to structure the discussion section: 1). Legal and ethical convergence; 2). Institutional responsibility and liability; 3). Cybersecurity maturity and regulation; 4). International harmonization and local adaptation.

This methodological design ensures that the review captures both global insights and context-specific challenges relevant to Indonesia's evolving digital health landscape.

RESULT AND DISCUSSION

An additional search using Publish or Perish software with Scopus-indexed filters was conducted to identify recent conference proceedings and empirical studies discussing cybersecurity issues in electronic medical records. The search produced three relevant documents:

Table 1. Articles From Scopus Database

Number	Authors	Title	Year	Source
1	Budiman	Preventing Cyber Crime in Electronic Medical Records Using Encryption Data	2023	1st International Conference on Technology, Engineering, and Computing Applications: Trends in Technology Development in the Era of Society 5.0, ICTECA 2023
2	A.K. Sekar	Emerging Cyber Security and Brute Force Attacks in Hospital Management Information Systems	2023	2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023
3	R. Sandhane	Cyber Security Risk Assessment for Electronic Medical Records (EMRs)	2024	4th International Conference on Innovative Practices in Technology and Management 2024, ICIPTM 2024

These studies illustrate the growing concern among computer scientists and systems engineers about the threat of cybercrime to electronic health data. However, while they offer important technological insights -such as the application of encryption Budiman (2023), brute-force attack prevention A. K. Sekar. (2023), and cybersecurity risk models R. Sandhane (2024) -they largely overlook legal and ethical implications. This technological emphasis confirms the phenomenon and research gaps identified earlier: although threats to EMRs from cybercrime are well acknowledged in technical literature, there is still a lack of integration with legal scholarship, especially regarding the rights of patients and the responsibilities of healthcare providers. Consequently, these studies support the need for more interdisciplinary legal research that addresses the regulatory and institutional mechanisms required to ensure accountability, informed consent, and legal compliance in digital health systems.

The results of a thematic content analysis based on a selection of 18 key documents—three retrieved via Scopus-indexed search using Publish or Perish, and 15 top-cited articles from Google Scholar. These studies were analyzed using four main themes that emerged consistently across the literature. These themes serve as the framework for discussing the role of cybercrime in shaping the legal and policy landscape of EMRs.

Table 2. Articles From Google-Scholar Database

Number	Cites	Authors	Title	Year	Source
1	1048	PSC MZ, R Sidi	Professional Ethics and Health Law in the Digital Era and the Challenges of Patient Medical Data Protection In Electronic Medical Record System	2025	International Conference on Artificial …
2	216	A Herisasono	Legal Liability of Health Care Facilities for Leakage of Patient Electronic Medical Records	2025	Pena Justisia: Media Komunikasi dan Kajian …
3	188	S Gupta, M Kapoor, SK Debnath	Cybersecurity Risks and Threats in Healthcare	2025	Artificial Intelligence-Enabled Security …
4	165	TM Anwar, JG Tambun, A Jaeni	Juridical Analysis Of The Misuse Of Electronic Medical Records In The Perspective Of The Electronic Information And …	2025	PRANATA HUKUM
5	144	P Eappen, V Gunn, HS Brar…	Capitalizing on the transformative role of AI and human capital to strengthen cybersecurity in healthcare	2025	… Intelligence and Cyber …
6	138	MF Rasyad, RL Lubis	Hospital Patient Data Security Evaluation to Achieve SDGs 3.8. 1 "Good Health and Wellbeing"	2025	Enrichment: Journal of …
7	106	R Sandhane, K Patil, AR Sharma	Cyber Security Risk Assessment for Electronic Medical Records (EMRs)	2024	2024 4th International …
8	96	L Gates	Cyber Attacks on Interoperable Electronic Health Records: A Clear and Present Danger	2024	Missouri Medicine
9	84	V Janarthanan, NV Nagrale, OG Singh, KV Raj…	Legal and Ethical Issues Associated With Challenges in the Implementation of the Electronic Medical Record System and Its Current Laws in India	2024	Cureus
10	83	S Jain, P Ashok, S Prabhu	Emerging Technologies for Cybersecurity in Healthcare: Evaluating Risks and Implementing Standards	2024	2024 International Conference on …
11	81	PC Yeh, KW Yeh, JL Huang	Security Risk Assessment for Patient Portals of Hospitals: A Case Study of Taiwan	2024	Risk Management and Healthcare …
12	75	S Monteith, T Glenn, JR Geddes…	Artificial intelligence and cybercrime: implications for individuals and the healthcare sector	2024	The British Journal of …
13	74	I Sukesti, E Sutrisno, SP Indraswari	Legal Study Of Electronic Medical Records For The Protection Of Patient Rights	2024	HERMENEUTIKA: Jurnal Ilmu …
14	70	G Mittal, S Mittal	Securing Healthcare Communication: Strategies for Email Security.	2024	IUP Journal of Information Technology
15	66	R Ibrahim, QA Al-Haija	Blockchain Security Measures to Combat Cyber Crime	2024	Cyber Security for Next-Generation …

Theme 1: Convergence Between Law and Ethics in EMR Governance

Several studies emphasize that legal protection for EMRs cannot be separated from ethical concerns. PSC MZ and R Sidi (2025) argue that the digitalization of health records creates new ethical dilemmas related to patient autonomy and data confidentiality P. S. C. MZ and R. Sidi. (2025). They stress the importance of aligning ethical codes of professional conduct with enforceable legal instruments. This convergence is critical, especially when healthcare professionals act as both data stewards and moral agents.

Other studies, such as those by Janarthanan et al. (2024), reinforce that EMR systems must ensure patient dignity and informed consent, even in a digital environment V. Janarthanan, N. V Nagrale, O. G. Singh, K. V Raj. (2024). This includes clearly communicating the risks of data sharing and the protocols for breach notifications. These findings highlight a shared responsibility between the legal system and professional health ethics to build trust in digital platforms.

Theme 2: Institutional Liability and the Limits of Risk Transfer

Legal liability for EMR breaches is a recurring concern across the literature. A. Herisasono (2025) explores how Indonesian hospitals may be held liable under civil and administrative law if patient data are leaked due to negligence A. Herisasono. (2025). The study calls for clearer mechanisms to determine institutional responsibility, particularly in public health facilities.

Indonesia use the UU ITE as a basis for juridical analysis, arguing that legal provisions on digital evidence and data misuse require reform to accommodate health-specific contexts S. Gupta, M. Kapoor, and S. K. Debnath (2025). Many authors argue that third-party IT vendors, while often tasked with managing EMR infrastructure, should not become loopholes for escaping liability. Risk transfer through outsourcing does not eliminate the hospital's fundamental duty to ensure data security.

Theme 3: Cybersecurity Maturity and Regulatory Enforcement

Several international contributions, analyze how systemic weaknesses in healthcare infrastructure expose EMRs to cybercrime S. Monteith, T. Glenn, J. R. Geddes. (2024), S. Gupta, M. Kapoor, and S. K. Debnath (2025). L. Gates. (2024). Their findings show that the maturity of a country's cybersecurity landscape correlates directly with the strength of its EMR protection laws.

Countries that integrate EMR protocols within their broader national cybersecurity strategies -like through the GDPR in the EU or HIPAA in the U.S.- have demonstrated better resilience. In contrast, studies on Indonesia, highlight the lack of digital readiness in achieving the SDGs related to health and wellbeing M. F. Rasyad and R. L. Lubis. (2025). Studies argue that healthcare institutions should adopt a "resilience-by-design" approach, including routine security audits, digital literacy training for health workers, and alignment of IT investment with legal risk assessments P. Eappen, V. Gunn, H. S. Brar (2025).

Theme 4: Harmonization of Legal Norms and Localization Challenges

Legal harmonization is a strong recommendation across the literature. Many authors advocate for aligning national laws with international standards such as GDPR and HIPAA. Indonesia must not only protect patient rights but also create interoperable frameworks that facilitate data exchange while maintaining legal safeguards I. Sukesti, E. Sutrisno, and S. P. Indraswari. (2024).

However, localization challenges are significant. A case study in Taiwan, note that imported standards often fail unless adapted to local institutional culture and regulatory capacity P. C. Yeh, K. W. Yeh, and J. L. Huang. (2024). This is supported by Ibrahim and Al-Haija (2024), who propose blockchain-based solutions that consider legal pluralism and local governance models R. Ibrahim and Q. A. Al-Haija. (2024).

Cross-Cutting Insight: Technology Outpacing Law

Across all themes, one meta-pattern stands out: the pace of technological innovation is outstripping the ability of legal frameworks to respond. Emerging technologies such as AI, blockchain, and predictive analytics are being deployed in EMRs without clear regulatory guidance . Study raise alarm about AI-generated decisions in healthcare that may impact legal accountability in the event of harm S. Monteith, T. Glenn, J. R. Geddes. (2024).

This thematic analysis confirms that cybercrime is both a technical and legal threat to health systems, with ripple effects for patient trust, professional conduct, and institutional accountability. The convergence of themes reveals a fragmented legal environment that urgently needs integration.

Implications for Indonesia and Similar Jurisdictions

For countries like Indonesia, these findings point to several urgent priorities in strengthening the governance of electronic medical records. First, there is a need to enhance cross-sectoral coordination among key state institutions, including the Ministry of Health, the Ministry of Communication and Informatics, and the Financial Supervisory Agency, particularly in areas of cyber risk monitoring and regulatory oversight. Second, Indonesia must develop specific legal instruments governing EMRs, which are currently underregulated, and integrate these with the newly enacted Personal Data Protection Law to ensure consistency in enforcement and scope. Third, it is imperative to establish a regulatory body or authority focused on e-health governance, equipped with investigative and audit powers to oversee compliance, enforce sanctions, and provide accountability in cases of data breach or misuse. Lastly, to strengthen institutional preparedness, healthcare professionals should be equipped with continuous education on digital ethics and cybersecurity law, ensuring that they are not only technically literate but also legally aware of their roles as data stewards.

The literature reviewed provides rich, multidimensional insights into the legal and ethical issues surrounding EMRs in the context of cybercrime. Four dominant themes -ethical-legal convergence, institutional liability, regulatory readiness, and legal harmonization -offer a robust framework to understand the current state of protection and its shortcomings. Future research and policy development should emphasize these themes to construct a more accountable and legally resilient digital health environment.

CONCLUSION

The rapid digitization of healthcare, while bringing considerable efficiency gains, also introduces profound legal and ethical challenges -especially in the form of rising cybercrime threats. This literature review has illuminated the multifaceted risks and gaps associated with the management of Electronic Medical Records (EMRs), particularly from the standpoint of patients' rights and the legal responsibilities of healthcare providers.

Thematic content analysis of 18 selected studies reveals four major areas of concern. First, legal and ethical frameworks often operate in parallel without integration, weakening the enforceability of patient protections in digital contexts. Second, the question of institutional liability remains inconsistently defined, particularly in health systems that rely on outsourced IT solutions without clear lines of accountability. Third, cybersecurity maturity varies greatly by jurisdiction, affecting how well EMR laws are implemented and enforced. Fourth, despite global efforts to harmonize standards (e.g., through GDPR and HIPAA), local adaptation is both essential and lacking in many developing contexts, including Indonesia.

From these findings, it is evident that EMR protection in Indonesia and similar jurisdictions demands not just technological responses, but also legislative reform and institutional restructuring. The law must keep pace with evolving cyber threats, and must proactively define the scope of patient rights, consent mechanisms, data access controls, and breach notification obligations.

In conclusion, safeguarding EMRs in the digital era is not solely a matter of data encryption or IT infrastructure- it is a question of legal resilience, institutional readiness, and ethical responsibility. The findings of this review underscore the need for an interdisciplinary and future-proof approach that bridges technology, law, and patient rights. Indonesia now stands at a critical juncture to lead in the development of inclusive, rights-based, and cyber-secure digital health governance.

REFERENCES

A. Booth, R. M. Purnagunawan, and ..., (2019). “Towards a healthy Indonesia?,” *Bulletin of Indonesian* doi: 10.1080/00074918.2019.1639509.

A. Herisasono. (2025). “Legal Liability of Health Care Facilities for Leakage of Patient Electronic Medical Records,” *Pena Justisia: Media Komunikasi dan Kajian* [Online]. Available: http://jurnal.unikal.ac.id/index.php/hk/article/view/5880

A. K. Sekar. (2023). “Emerging Cyber Security and Brute Force Attacks in Hospital Management Information Systems,” *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, pp. 421–426, 2023, doi: 10.1109/SmartTechCon57526.2023.10391825.

A. Rollins. (2016)“Health’prime target’for cybercrime,” *Australian Medicine*, 2016, doi: 10.3316/ielapa.485275547674158.

A. Wirth. (2011). “Cybercrimes pose growing threat to medical devices,” *Biomedical instrumentation &technology*, doi: 10.2345/0899-8205-45.1.26.

B. Yuan and J. Li. (2019) “The policy effect of the general data protection regulation (GDPR) on the digital public health sector in the european union: An empirical investigation,” *Int J Environ Res Public Health*, vol. 16, no. 6, doi: 10.3390/ijerph16061070.

Budiman. (2023). “Preventing Cyber Crime in Electronic Medical Records Using Encryption Data,” *1st International Conference on Technology, Engineering, and Computing Applications: Trends in Technology Development in the Era of Society 5.0, ICTECA* doi: 10.1109/ICTECA60133.2023.10490705.

C. George and B. Berčič. (2009). “Electronic medical records: addressing privacy &security concerns in the UK and US,” *BILETA To Infinity and Beyond: Law and ...*, [Online]. Available: https://repository.mdx.ac.uk/item/82934

C. Santos. (2020). *Medical Identity Theft: A Cybercrime*. search.proquest.com, 2020. [Online]. Available: https://search.proquest.com/openview/cbd95688ad019914884303fc68d90752/1?pq-origsite=gscholar&cbl=18750&diss=y

D. Dhingra and A. Dabas. (2020). “Global Strategy on Digital Health,” *Indian Pediatr*, vol. 57, no. 4, 2020, doi: 10.1007/s13312-020-1789-7.

F. Pazarcıkcı, N. Karataş, and A. Kaya (2024). “The relationships of parents’ mental well-being and sociodemographic characteristics with digital parenting awareness: Structural equation model analysis,” *J Pediatr Nurs*, vol. 75, doi: 10.1016/j.pedn.2023.12.036.

Hassan Samkari and Adnan Gutub, (2015). “Protecting Medical Records against Cybercrimes within Hajj Period by 3-layer Security,” *Recent Trends in Information Technology and Its Application*, vol. 2, no. 3, 2019, doi: 10.5281/zenodo.3543455.

I. Sukesti, E. Sutrisno, and S. P. Indraswari. (2024) “LEGAL STUDY OF ELECTRONIC MEDICAL RECORDS FOR THE PROTECTION OF PATIENT RIGHTS,” *HERMENEUTIKA:* [Online]. Available: https://ejournalugj.com/index.php/HERMENEUTIKA/article/view/9588

J. Li and M. J. Shaw. (2012). “Safeguarding the Privacy of Electronic Medical Records,” *Cyber Crime: Concepts, Methodologies, Tools and …*, [Online]. Available: https://www.igi-global.com/chapter/content/60987

J. N. Weiss. (2023). “The Health Insurance Portability and Accountability Act (HIPAA),” in *Physician Crisis*, 2023. doi: 10.1007/978-3-031-27979-9_15.

J. Villalobos and N. Calvanese. (2021). “The impact of COVID-19 pandemic on doctor-patient relationship,” *Rev Med Chil*, vol. 149, no. 7, doi: 10.4067/S0034-98872021000701070.

L. Gates. (2024). “Cyber Attacks on Interoperable Electronic Health Records: A Clear and Present Danger,” *Mo Med*, [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC10887471/

M. F. Rasyad and R. L. Lubis. (2025). “Hospital Patient Data Security Evaluation to Achieve SDGs 3.8. 1 ‘Good Health and Wellbeing,’” *Enrichment: Journal of* [Online]. Available: http://journalenrichment.com/index.php/jr/article/view/326

M. K. Hossain, J. Sutanto, P. W. Handayani, A. A. Haryanto, J. Bhowmik, and V. Frings-Hessami. (2025). “An exploratory study of electronic medical record implementation and recordkeeping culture: the case of hospitals in Indonesia,” *BMC Health Serv Res*, doi: 10.1186/s12913-025-12399-0.

M. S. Anker, S. Hadzibegovic, A. Lena, and W. Haverkamp. (2019). “The difference in referencing in Web of Science, Scopus, and Google Scholar,” *ESC Heart Fail*, vol. 6, no. 6, 2019, doi: 10.1002/ehf2.12583.

M. Sumarto and A. Kaasch, (2018). *New directions in social policy evidence from the Indonesian Health Insurance Programme*. econstor.eu, [Online]. Available: https://www.econstor.eu/handle/10419/207012

M. Zimoń and R. Kasprzyk. (2021). “Digital revolution and cyber threats as its consequence,” *Proceedings of the 38th International Business …*, [Online]. Available: https://www.researchgate.net/profile/Rafal-Kasprzyk/publication/357657126_Digital_revolution_and_cyber_threats_as_its_consequence/links/61d8453dd45006081694d2cb/Digital-revolution-and-cyber-threats-as-its-consequence.pdf

N. Amalia, M. Z. Azhri, A. Rosarini, D. R. Wijayanti, and M. A. Riestiyowati, (2021) “The Implementation of Electronic Medical Record (EMR) in The Development Health Care System in Indonesia: A Literature Review,” *International Journal of Advancement in Life Sciences Research*, vol. 4, no. 3, 2021, doi: 10.31632/ijalsr.2021.v04i03.002.

P. C. Yeh, K. W. Yeh, and J. L. Huang. (2024). “Security Risk Assessment for Patient Portals of Hospitals: A Case Study of Taiwan,” *Risk Management and Healthcare* doi: 10.2147/RMHP.S463408.

P. Eappen, V. Gunn, H. S. Brar (2025). “Capitalizing on the transformative role of AI and human capital to strengthen cybersecurity in healthcare,” … *Intelligence and Cyber* [Online]. Available: https://books.google.com/books?hl=en&lr=&id=7URUEQAAQBAJ&oi=fnd&pg=PA112&dq=emr+cyber+crime&ots=0Rh-gFSanr&sig=MrjjR3FLqg7njco0cTKj9yCgvrQ

P. S. C. MZ and R. Sidi. (2025).“Professional Ethics and Health Law in the Digital Era and the Challenges of Patient Medical Data Protection In Electronic Medical Record System,” *International Conference on Artificial* [Online]. Available: https://www.icaneat-apibanyuwangi.org/index.php/icaneat/article/view/109

R. G. Smith. (2015). “Trajectories of cybercrime,” *Cybercrime risks and responses: Eastern and western …*, doi: 10.1057/9781137474162_2.

R. Ibrahim and Q. A. Al-Haija. (2024). “Blockchain Security Measures to Combat Cyber Crime,” *Cyber Security for Next-Generation*, doi: 10.1201/9781003404361-15.

R. Pranckutė, “Web of Science (WoS) and Scopus: the titans of bibliographic information in today’s academic world,” 2021. doi: 10.3390/publications9010012.

R. Sandhane. (2024). “Cyber Security Risk Assessment for Electronic Medical Records (EMRs),” *4th International Conference on Innovative Practices in Technology and Management 2024, ICIPTM 2024*, 2024, doi: 10.1109/ICIPTM59628.2024.10563486.

S. Ghosh and E. Turrini. (2010) *Cybercrimes: a multidisciplinary analysis*. books.google.com, [Online]. Available: https://books.google.com/books?hl=en&lr=&id=aFJqtsfQhSkC&oi=fnd&pg=PR5&dq=emr+cyber+crime&ots=CuZZ_2Tw71&sig=g4D_njtAHuvpiYDpxTsO-92x2WM

S. Gupta, M. Kapoor, and S. K. Debnath (2025). “Cybersecurity Risks and Threats in Healthcare,” *Artificial Intelligence-Enabled Security* doi: 10.1007/978-3-031-82810-2_3.

S. John, N. Ravichandran, and M. F. Khan. (2018). “Electronic medical record for deliverance of effective healthcare delivery: Ethical issues and challenges of digitalization in clinical information and Electronic …,” *IOSR Journal of Business and* [Online]. Available: https://www.academia.edu/download/56830066/A2003020106.pdf

S. Monteith, T. Glenn, J. R. Geddes. (2024). “Artificial intelligence and cybercrime: implications for individuals and the healthcare sector,” *The British Journal of …*, 2024, [Online]. Available: https://www.cambridge.org/core/journals/the-british-journal-of-psychiatry/article/artificial-intelligence-and-cybercrime-implications-for-individuals-and-the-healthcare-sector/6409A9AB77FE31DD8033D7B761D20381

S. Sutardi and L. Ferdiles. (2023). “Law Enforcement Against Cybercrime in Online Activities,” *... Ilmu Sosial dan* [Online]. Available: https://edunity.publikasikupublisher.com/index.php/Edunity/article/view/34

S. Thakral and A. Vaish. (2022). “CYBER SMART: PROTECT THE PATIENT; PROTECT THE DATA ON ELECTRONIC MEDICAL RECORD,” *academia.edu*, [Online]. Available: https://www.academia.edu/download/117285535/ijtrs.v07.i01.pdf

S. Xu, J. Ning, Y. Li, Y. Zhang, G. Xu, (2021).“A secure EMR sharing system with tamper resistance and expressive access control,” ... *on Dependable and* [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9609621/

T. M. Anwar, J. G. Tambun, and A. Jaeni. (2025). “JURIDICAL ANALYSIS OF THE MISUSE OF ELECTRONIC MEDICAL RECORDS IN THE PERSPECTIVE OF THE ELECTRONIC INFORMATION AND …,” *PRANATA HUKUM*, [Online]. Available: https://jurnalpranata.ubl.ac.id/index.php/pranatahukum/article/view/380

V. Janarthanan, N. V Nagrale, O. G. Singh, K. V Raj. (2024). “Legal and Ethical Issues Associated With Challenges in the Implementation of the Electronic Medical Record System and Its Current Laws in India,” *Cureus*, 2024, [Online]. Available: https://www.cureus.com/articles/207054-legal-and-ethical-issues-associated-with-challenges-in-the-implementation-of-the-electronic-medical-record-system-and-its-current-laws-in-india.pdf

V. Popa *et al.*, (2024)“Delivering Digital Health Solutions that Patients Need: A Call to Action,” doi: 10.1007/s43441-023-00592-4.

Y. K. WINDI. (2018)“An Emerging Health Protection System and Its Coverage of A Vulnerable and Marginalised Population: The Waste Pickers of Surabaya, Indonesia,” *scholar.archive.org*. [Online]. Available: https://scholar.archive.org/work/i7jqhylk7jds7dizqfmjvebhh4/access/wayback/https://au-east.erc.monash.edu.au/fpfiles/11080613/YohanesKWindiFinalThesis.pdf