Customary Law Journal, AICOPS Special Collection 2026, *Page*: 1-18

Medical Data Leakage in Healthcare: A Systematic Literature Review of Cybersecurity, Legal Issues, and Patient Privacy

Ade Netra Kartika*, Ahmad Redi

Faculty of Law, Universitas Borobudur, Jakarta; ade_netra@yahoo.com
Faculty of Law, Universitas Borobudur, Jakarta; ahmad_redi@borobudur.ac.id

DOI:
https://doi.org/10.47134/jcl.v3i3.2.6333
*Correspondence: Ade Netra Kartika
Email: ade_netra@yahoo.com

Received: 08/08/2026
Accepted: 29/08/2026
Published: 31/08/2026

Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY-SA) license (http://creativecommons.org/licenses/by-sa/4.0/).

Abstract: *Medical data leakage has become one of the most critical challenges facing healthcare organizations as digital health technologies, electronic health records (EHRs), artificial intelligence, cloud computing, and interconnected medical devices continue to expand. Beyond compromising sensitive patient information, data leakage threatens patient safety, institutional trust, and regulatory compliance. This study systematically reviews the existing literature to examine the causes, consequences, legal implications, and prevention strategies of medical data leakage in healthcare. A Systematic Literature Review (SLR) following the PRISMA 2020 guidelines was conducted. The literature was identified through Scopus and PubMed, using a structured search strategy based on predefined keywords and Boolean operators. The search was supplemented by backward and forward reference checking of the eligible studies to identify potentially relevant publications. Fourteen peer-reviewed studies that met the predefined eligibility criteria were included in the thematic synthesis. The retrieved studies were analyzed using evidence mapping, thematic coding, quality appraisal, and narrative synthesis. Three major analytical domains emerged from the analysis: (1) healthcare cybersecurity vulnerabilities, (2) medical data leakage pathways and patient privacy consequences, and (3) legal protection and healthcare governance. The findings indicate that medical data leakage is not solely a technical cybersecurity issue but results from the interaction of technological vulnerabilities, human behavior, organizational governance, and regulatory implementation. The review proposes an integrated thematic synthesis framework linking cybersecurity vulnerabilities, medical data leakage pathways, legal protection, and governance responses to strengthen healthcare cyber resilience. The findings provide practical implications for healthcare organizations, policymakers, and researchers in developing comprehensive strategies for protecting medical information in an increasingly digital healthcare environment.*

Keywords: *medical data leakage; healthcare cybersecurity; patient privacy; legal protection; healthcare governance; systematic literature review.*

Introduction

Healthcare systems worldwide are undergoing an unprecedented digital transformation driven by the rapid adoption of Electronic Health Records (EHRs), telemedicine, artificial intelligence (AI), cloud computing, wearable medical devices, and the Internet of Medical Things (IoMT) (Dehghan et al., 2026). These technologies have significantly improved healthcare accessibility, clinical decision-making, operational efficiency, and continuity of patient care. Digital health technologies enable healthcare providers to exchange patient information in real time, support data-driven diagnosis, facilitate remote healthcare services, and improve overall healthcare quality. As

governments and healthcare organizations continue to promote digital health ecosystems, medical information has become one of the most valuable strategic assets in modern healthcare systems.

Despite these benefits, healthcare digitalization has simultaneously expanded cybersecurity risks and increased the frequency of medical data leakage (Subekti, 2024). Healthcare organizations have become one of the most attractive targets for cybercriminals because they store extensive amounts of sensitive personal information, including demographic profiles, medical histories, laboratory results, imaging records, prescription data, insurance information, and increasingly, genomic information. Unlike financial information that can often be replaced after compromise, medical records are permanent and may be exploited for identity theft, insurance fraud, blackmail, illegal medical transactions, and social engineering attacks. Consequently, medical data breaches have become one of the most significant cybersecurity challenges confronting healthcare systems worldwide.

The increasing number of healthcare cyber incidents demonstrates that technological advancement alone does not guarantee data security (Desai & Desai, 2023). Recent reports indicate that ransomware attacks, phishing campaigns, insider misuse, cloud misconfigurations, third-party service providers, legacy information systems, and weak authentication mechanisms remain dominant causes of medical data breaches. These incidents not only compromise the confidentiality, integrity, and availability of health information but also disrupt clinical services, delay medical treatment, increase operational costs, and threaten patient safety. The systematic review by Ewoh and Vartiainen identified five major sources of healthcare cybersecurity vulnerability: human error, inadequate cybersecurity investment, complex interconnected medical devices, legacy systems, and the rapid pace of digital transformation, highlighting that cybersecurity challenges are socio-technical rather than purely technological (Ewoh & Vartiainen, 2024).

The consequences of medical data leakage extend far beyond financial losses (Seh et al., 2020). Data breaches may erode patients' trust in healthcare institutions, discourage individuals from disclosing sensitive medical information, and ultimately reduce the quality of healthcare services. From an organizational perspective, healthcare providers may experience reputational damage, operational disruption, regulatory investigations, litigation, and substantial recovery costs following a major cyber incident. Large-scale attacks on healthcare organizations during recent years have demonstrated that even highly developed healthcare infrastructures remain vulnerable to sophisticated cyber threats .

Besides cybersecurity concerns, medical data leakage has become an increasingly important legal and governance issue. Medical information is universally recognized as highly sensitive personal data because it directly relates to an individual's health condition, dignity, and fundamental rights. Consequently, many countries have strengthened legal frameworks governing healthcare data protection. Within the European Union, the General Data Protection Regulation (GDPR) establishes strict obligations regarding lawful processing, informed consent, breach notification, accountability, and patients' rights over personal data (Hoofnagle et al., 2019). In the United States, the Health Insurance Portability and Accountability Act (HIPAA) and its subsequent amendments regulate the privacy and

security of protected health information (Tovino, 2025). Indonesia has also strengthened legal protection through Law Number 27 of 2022 concerning Personal Data Protection and Law Number 17 of 2023 concerning Health, which recognize health data as sensitive personal data requiring enhanced protection (Budiman, 2023). Nevertheless, legal compliance alone has not been sufficient to significantly reduce the frequency of healthcare data breaches, suggesting that regulatory compliance must be complemented by effective governance, organizational preparedness, and continuous cybersecurity improvement.

Another emerging challenge concerns the rapid integration of artificial intelligence into healthcare services. AI-based clinical decision support systems, predictive analytics, large language models, and machine learning applications require extensive datasets to improve diagnostic accuracy and healthcare delivery. While these technologies offer considerable clinical benefits, they simultaneously increase concerns regarding unauthorized data access, secondary use of medical information, algorithmic transparency, data ownership, cross-border data transfers, and accountability for automated decision-making. The integration of AI therefore requires healthcare organizations to balance innovation with patient privacy, cybersecurity, ethical principles, and regulatory compliance (Ahmed, 2025), (Munoko & others, 2023) Previous studies have examined various aspects of healthcare cybersecurity (Seh et al., 2020), including ransomware attacks, electronic health records (McMullen et al., 2014), (Keith Mweebo, 2014), (Hossain et al., 2025), (MULUKUNTLA, 2015), blockchain implementation (Zakzouk et al., 2023), (Lee et al., 2021), (Ettaloui et al., 2024), federated learning, cloud security, and patient privacy. Several review articles have also discussed cybersecurity challenges in healthcare from technical or sociotechnical perspectives. However, the existing literature remains fragmented because most reviews concentrate on specific technologies or particular cybersecurity threats. Comparatively fewer studies integrate technological vulnerabilities, legal protection, patient privacy, and healthcare governance within a single comprehensive review. Such fragmentation limits the ability of researchers, policymakers, and healthcare practitioners to understand medical data leakage from an interdisciplinary perspective and to identify comprehensive strategies for protecting patient information.

Furthermore, the increasing complexity of digital healthcare ecosystems necessitates a broader perspective that extends beyond information technology. Effective protection of medical information requires collaboration among healthcare professionals, information technology specialists, legal experts, policymakers, hospital administrators, and patients themselves. Data leakage should therefore be understood not merely as a technical failure but also as a governance, legal, ethical, and organizational challenge. This broader perspective is particularly relevant for countries currently accelerating digital health transformation while simultaneously strengthening personal data protection regulations.

Based on these considerations, this study conducts a Systematic Literature Review (SLR) following the PRISMA 2020 guidelines to synthesize recent evidence regarding medical data leakage in healthcare (Page et al., 2021). Specifically, this review aims to (1) identify the primary causes of medical data leakage, (2) examine legal and regulatory issues related to patient data protection, (3) review technological and organizational strategies for preventing healthcare data breaches, and (4) identify future research directions for strengthening healthcare cybersecurity and governance. By integrating evidence from

cybersecurity, legal studies, and healthcare management, this review provides a comprehensive overview of the current state of knowledge and offers practical implications for researchers, healthcare organizations, and policymakers seeking to improve the protection of sensitive medical information.

Research Questions

Based on the identified research gap, this study addresses the following research questions:

RQ1: What are the major causes of medical data leakage in healthcare organizations?

RQ2: What legal and regulatory frameworks have been discussed in the literature to protect medical data?

RQ3: What future research directions can strengthen healthcare cybersecurity, patient privacy, and legal protection?

Literature Review

Digital Healthcare and Medical Data

The healthcare sector has undergone significant digital transformation over the past decade. The implementation of Electronic Health Records (EHRs), Electronic Medical Records (EMRs), telemedicine, cloud computing, artificial intelligence (AI), mobile health (mHealth), and the Internet of Medical Things (IoMT) has fundamentally changed the way healthcare services are delivered. These technologies facilitate timely access to patient information, improve diagnostic accuracy, enhance communication among healthcare providers, and support evidence-based clinical decision-making (Ewoh & Vartiainen, 2024).

Medical data constitute one of the most valuable and sensitive categories of personal information because they contain comprehensive records of an individual's physical and mental health status (S. J. Nass and O. L. Levit, 2014). Such information includes patient identity, demographic characteristics, medical history, laboratory results, diagnostic images, prescriptions, insurance information, genetic information, and treatment records. Unlike financial information, medical records cannot easily be replaced after exposure, making their protection essential for both healthcare providers and patients (Chiruvella & Guddati, 2021).

Indonesia has also accelerated healthcare digitalization through the implementation of Electronic Medical Records as part of the national health transformation agenda. The Ministry of Health Regulation No. 24 of 2022 concerning Medical Records requires healthcare facilities to gradually implement electronic medical record systems to improve healthcare quality and service efficiency. While this transformation creates significant opportunities for integrated healthcare services, it also increases cybersecurity risks and raises concerns regarding the protection of patients' personal data (Nugroho, 2021).

Consequently, protecting medical information has become a strategic priority in digital healthcare. Effective protection requires not only technological safeguards but also organizational governance, legal compliance, and continuous risk management.

Medical Data Leakage

Medical data leakage refers to the unauthorized access, disclosure, acquisition, modification, or dissemination of healthcare information without appropriate authorization

(J. Starcke, J. Spadafora, J. Spadafora, P. Spadafora, 2025), (Budiono et al., 2024), (Shi et al., 2025). Data leakage may occur intentionally through cyberattacks or unintentionally because of human error, system failures, or inadequate security practices. Because medical information possesses high economic and social value, healthcare organizations have increasingly become attractive targets for cybercriminals.

Previous studies identify several major causes of healthcare data leakage. Technical factors include ransomware attacks, malware, phishing, insecure application programming interfaces (APIs), cloud misconfiguration, legacy systems, and software vulnerabilities. Organizational factors include inadequate cybersecurity governance, insufficient employee awareness, poor password management, weak authentication mechanisms, and ineffective vendor management. Human error remains one of the most frequently reported causes of healthcare data breaches, indicating that cybersecurity is not solely a technological issue but also an organizational and behavioral challenge (Ewoh & Vartiainen, 2024), (Ewoh et al., 2025).

The consequences of medical data leakage are multidimensional. Besides financial losses, healthcare organizations may experience operational disruption, legal sanctions, reputational damage, and declining public trust. More importantly, compromised medical information may threaten patient safety by delaying treatment, reducing information accuracy, or interrupting healthcare delivery during cyber incidents.

Patient Privacy

Patient privacy represents a fundamental principle of healthcare ethics and an essential component of quality healthcare services. Confidentiality encourages patients to disclose accurate medical information, enabling healthcare professionals to provide appropriate diagnosis and treatment. Without adequate privacy protection, patients may become reluctant to seek healthcare services or disclose sensitive medical conditions, ultimately affecting healthcare quality

Digital transformation has substantially increased privacy challenges because healthcare information is routinely exchanged among hospitals, laboratories, insurance companies, cloud service providers, pharmaceutical companies, and telemedicine platforms. Furthermore, secondary uses of medical data for research, artificial intelligence development, and healthcare analytics have generated additional concerns regarding patient consent, transparency, and data ownership.

Recent literature emphasizes that patient privacy should not be viewed exclusively as a technological issue. Rather, effective privacy protection requires an integrated approach involving legal compliance, ethical principles, organizational governance, staff awareness, and institutional accountability. Continuous employee training and clear organizational policies remain essential components of healthcare privacy protection

Legal Protection of Medical Data

The increasing frequency of healthcare data breaches has prompted governments worldwide to strengthen legal frameworks for protecting personal health information. Because health information directly relates to an individual's physical and mental condition, it is generally classified as sensitive personal data requiring enhanced legal protection.

In Indonesia, legal protection of medical information has significantly improved following the enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) and Law No. 17 of 2023 concerning Health. The PDP Law explicitly recognizes health information as specific personal data requiring stronger legal protection. Furthermore, Ministry of Health Regulation No. 24 of 2022 concerning Medical Records requires healthcare facilities to implement Electronic Medical Records while ensuring confidentiality, integrity, and availability of patient information.

Previous review studies have extensively discussed healthcare cybersecurity, blockchain applications, artificial intelligence, ransomware mitigation, electronic health records, and patient privacy. However, most of these reviews focus primarily on technological solutions while providing limited discussion of legal protection and governance issues.

Furthermore, studies conducted in Indonesia predominantly adopt normative legal approaches examining the implementation of the Personal Data Protection Law, Health Law, and Electronic Medical Records Regulation. Conversely, international studies tend to emphasize cybersecurity technologies, artificial intelligence, cloud security, blockchain, and zero-trust architectures. As a result, limited evidence is available regarding the integration of technological, legal, governance, and patient privacy perspectives within a single systematic review.

Methodology

This study employed a Systematic Literature Review (SLR) to synthesize existing knowledge on medical data leakage in healthcare, with particular attention to cybersecurity, legal protection, and patient privacy. The review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines to ensure transparency, reproducibility, and methodological rigor throughout the review process (Page et al., 2021). The literature search was conducted using Scopus and PubMed, two internationally recognized databases that comprehensively index peer-reviewed publications in medicine, health informatics, cybersecurity, information systems, and health law. The literature search was performed in January 2026, focusing on studies published between 2020 and 2025 to capture recent developments in digital healthcare technologies, cybersecurity threats, and data protection regulations.

To identify relevant studies, combinations of keywords related to medical data protection were developed using Boolean operators. The search string included the terms *"medical data leakage"*, *"healthcare data breach"*, *"patient privacy"*, *"electronic health records"*, and *"medical information security"*, combined with keywords such as *cybersecurity*, *"legal protection"*, *GDPR*, *HIPAA*, *blockchain*, and *"artificial intelligence"*. The search strategy was refined iteratively to ensure comprehensive coverage while maintaining the relevance of retrieved publications.

After completing the database search, all identified records were exported and screened following the four stages recommended in the PRISMA 2020 framework: identification, screening, eligibility, and inclusion (Page et al., 2021). During the identification stage, duplicate records retrieved from different databases were removed. The remaining studies were screened based on their titles and abstracts to assess their relevance

to the objectives of this review. Studies unrelated to healthcare, patient privacy, medical information security, or legal protection of health data were excluded.

Result and Discussion

Table 1. Characteristics of Studies Included in the Preliminary Systematic Literature Review

No.	Author(s)	Year	Journal	Study Design	Main Focus	Key Findings
1	Ewoh & Vartiainen	2024	*Journal of Medical Internet Research*	Systematic Review	Healthcare cybersecurity vulnerabilities	Cybersecurity vulnerabilities arise from interactions among technological, organizational, and human factors, requiring sociotechnical solutions.
2	Nemec Zlatolas, Welzer, & Lhotska	2024	*Cluster Computing*	Review	Security mechanisms for healthcare data breaches	Encryption, authentication, blockchain, and AI are among the most frequently proposed mechanisms for mitigating healthcare data breaches.
3	Subramanian, Sengupta, & Xu	2024	*Journal of Medical Internet Research*	Mixed-methods	Patient health record protection	Legal compliance alone does not eliminate healthcare data breaches; organizational governance remains essential.
4	Baines et al.	2024	*Journal of Medical Internet Research*	Systematic Review	Secondary use of health data	Trust, transparency, and dynamic consent strongly influence willingness to share personal health information.
5	Elendu et al.	2024	*Medicine*	Narrative Review	Legal implications of cybersecurity	Clinicians and healthcare organizations face increasing legal and ethical responsibilities related to cybersecurity incidents.*
6	Hasegawa et al.	2024	*Journal of Medical Internet Research*	Scoping Review	Cybersecurity interventions	Resource limitations affect cybersecurity implementation; governance and organizational preparedness remain critical.
7	Seh et al.	2020	*Healthcare*	Empirical Analysis	Healthcare data breaches	Healthcare data breaches continue to increase, with hacking and unauthorized access among the leading causes.
8	Bani Issa et al.	2020	*International Nursing Review*	Mixed-methods	Electronic health record privacy	Healthcare professionals reported concerns regarding confidentiality, unauthorized access, and inconsistent security policies.
9	Jalali et al.	2020	*Journal of Medical Internet Research*	Quantitative Study	Phishing behavior	Workload influenced phishing susceptibility more strongly than stated compliance intentions.
10	Li	2023	*Journal of Medical Internet Research*	Viewpoint	AI chatbot security	AI introduces new privacy risks through data input, storage, reuse, and model training.
11	Burke et al.	2024	*BMC Medical Informatics and Decision Making*	Qualitative Study	Cybersecurity self-evaluation	Healthcare organizations require sector-specific cybersecurity self-assessment and preparedness strategies.
12	Looi et al.	2024	*Australasian Psychiatry*	Practice Framework	Post-breach communication	Timely communication and psychological support are important after healthcare data breaches.*
13	Walden et al.	2020	*Health Security*	Empirical Study	Breach reporting	Reporting decisions are influenced by organizational knowledge, experience, and regulatory understanding.*
14	Almaghrabi & Bugis	2022	Healthcare cybersecurity literature	Review	EHR confidentiality	Security culture, access control, and retention policies are central to protecting electronic health records.*

Healthcare Cybersecurity Vulnerabilities

The reviewed literature consistently identifies healthcare organizations as one of the most vulnerable sectors to cyberattacks because of their extensive reliance on digital health technologies, interconnected medical devices, and electronic health records (EHRs). Rather than attributing cybersecurity incidents solely to technological weaknesses, the reviewed studies demonstrate that vulnerabilities emerge from interactions among technological infrastructure, organizational governance, and human behavior.

Another recurring issue concerns aging healthcare infrastructure. Many hospitals continue operating legacy systems that cannot easily be upgraded because of financial limitations, interoperability challenges, and the need to maintain uninterrupted clinical services. Consequently, healthcare organizations often experience simultaneous technological, organizational, and financial vulnerabilities, making them attractive targets for cybercriminals.

Medical Data Leakage and Patient Privacy

The reviewed studies indicate that medical data leakage extends beyond conventional cyberattacks. Three principal forms of data leakage emerged from the evidence synthesis: malicious cyber breaches**,** unauthorized access or disclosure**,** and secondary use of personal health information beyond its original purpose. Each pathway involves different actors, governance mechanisms, and legal implications.

Traditional cyber incidents such as ransomware, hacking, phishing, malware, and unauthorized system intrusion remain the most frequently discussed forms of healthcare data leakage. However, several studies emphasize that legitimate access to health information may also result in privacy violations when patient information is disclosed to unauthorized individuals or reused for purposes that were not originally consented to.

These findings indicate that protecting medical information requires more than preventing external cyberattacks. Healthcare organizations must also establish governance mechanisms that regulate who may access patient information, under what circumstances, for what purposes, and for how long. Consequently, patient privacy should be understood as an organizational governance issue rather than merely a technical security problem.

Across the fourteen included studies, the evidence indicates that medical data leakage should be distinguished according to its principal pathway. First, leakage may arise from malicious external attacks, including ransomware, hacking, phishing, malware, and unauthorized system intrusion. Second, leakage may result from internal or authorized-access failures, including credential misuse, insider disclosure, inadequate access controls, and inappropriate data sharing. Third, leakage may occur through the secondary use of health information, particularly when data are reused for research, artificial intelligence development, analytics, or commercial purposes beyond the scope originally communicated to the data subject. This distinction is analytically important because each pathway involves different actors, risks, legal obligations, and governance responses.

Interpretive Discussion: Comparative Legal Protection and Healthcare Governance

Legal protection represents a central dimension of the governance of medical information. However, the comparative value of legal frameworks should not be assessed merely by listing the existence of HIPAA, GDPR, or national personal data protection legislation. A more systematic comparison requires examination of the substantive obligations imposed on healthcare organizations and data controllers.

First, consent and lawful processing differ in their regulatory structure. The GDPR emphasizes lawful bases for processing, explicit protection for special categories of personal data, purpose limitation, and conditions governing the processing of health information. HIPAA, by contrast, regulates the use and disclosure of protected health information through a sector-specific framework applicable to covered entities and business associates. Indonesia's Law No. 27 of 2022 concerning Personal Data Protection recognizes health information as specific personal data requiring enhanced protection, while Law No. 17 of 2023 concerning Health and Ministry of Health Regulation No. 24 of 2022 provide additional sectoral obligations relating to medical information and electronic medical records.

Second, breach notification and organizational accountability constitute a major point of comparison. GDPR-based governance emphasizes accountability and formal obligations associated with personal data breaches, whereas the HIPAA framework establishes sector-specific obligations concerning the protection and disclosure of protected health information. The Indonesian framework increasingly recognizes institutional responsibility for the protection of personal data, although the effectiveness of implementation depends substantially on institutional capacity, internal governance, and enforcement mechanisms.

Third, the regulation of secondary data use and cross-border processing is particularly significant in digital healthcare. Health information may be transferred to cloud providers, artificial intelligence developers, research institutions, analytics companies, and other third parties. Legal protection must therefore extend beyond the initial healthcare provider and address purpose limitation, transparency, contractual safeguards, third-party accountability, and conditions governing international data transfers.

Fourth, liability and sanctions should be analyzed as part of an integrated governance system. Legal sanctions may provide deterrence, but effective prevention also depends on institutional accountability, incident documentation, internal reporting mechanisms, cybersecurity investment, vendor management, and the ability of patients to understand and exercise their rights. The comparative analysis therefore supports the conclusion that legal protection cannot operate effectively as an isolated compliance mechanism but must be embedded within the broader governance architecture of healthcare organizations.

Healthcare Cybersecurity Vulnerabilities

The reviewed literature consistently identifies healthcare organizations as one of the most vulnerable sectors to cyberattacks because of their extensive reliance on digital health technologies, interconnected medical devices, and electronic health records (EHRs). Rather than attributing cybersecurity incidents solely to technological weaknesses, the reviewed

studies demonstrate that vulnerabilities emerge from interactions among technological infrastructure, organizational governance, and human behavior.

Ewoh and Vartiainen identified five recurring sources of vulnerability across healthcare organizations: human error, inadequate cybersecurity investment, legacy information systems, interconnected endpoint devices, and rapid digital transformation (Ewoh & Vartiainen, 2024). Their systematic review argues that cybersecurity should be approached from a sociotechnical perspective because cyber incidents are rarely caused by a single technical failure. Instead, weaknesses in organizational processes, staff capability, and technology interact to increase the likelihood of successful cyberattacks.

The importance of human factors is further supported by empirical evidence. Hospital employees' actual phishing behavior was associated with workload and organizational conditions rather than merely their intention to comply with information security policies[26]. Likewise, Bani Issa et al. reported that healthcare professionals expressed concerns regarding unauthorized access to EHRs, insufficient cybersecurity training, and inconsistent organizational security policies. These findings collectively suggest that healthcare cybersecurity should be considered an organizational capability rather than solely an information technology function.

Another recurring issue concerns aging healthcare infrastructure. Many hospitals continue operating legacy systems that cannot easily be upgraded because of financial limitations, interoperability challenges, and the need to maintain uninterrupted clinical services. Consequently, healthcare organizations often experience simultaneous technological, organizational, and financial vulnerabilities, making them attractive targets for cybercriminals.

Medical Data Leakage and Patient Privacy

The reviewed studies indicate that medical data leakage extends beyond conventional cyberattacks. Three principal forms of data leakage emerged from the evidence synthesis: malicious cyber breaches**,** unauthorized access or disclosure**,** and secondary use of personal health information beyond its original purpose. Each pathway involves different actors, governance mechanisms, and legal implications.

Traditional cyber incidents such as ransomware, hacking, phishing, malware, and unauthorized system intrusion remain the most frequently discussed forms of healthcare data leakage. However, several studies emphasize that legitimate access to health information may also result in privacy violations when patient information is disclosed to unauthorized individuals or reused for purposes that were not originally consented to.

These findings indicate that protecting medical information requires more than preventing external cyberattacks. Healthcare organizations must also establish governance mechanisms that regulate who may access patient information, under what circumstances, for what purposes, and for how long. Consequently, patient privacy should be understood as an organizational governance issue rather than merely a technical security problem.

Legal Protection and Healthcare Governance

Legal protection represents another dominant theme emerging from the reviewed literature. Most studies discuss the role of regulatory frameworks such as the Health

Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe (Ettaloui et al., 2024). More recent publications also emphasize breach notification, institutional accountability, professional responsibility, and organizational governance.

The reviewed evidence suggests that regulatory compliance alone does not eliminate healthcare data breaches. Studies examining HIPAA implementation indicate that healthcare organizations may remain vulnerable despite compliance with existing regulations because legal compliance does not necessarily guarantee effective cybersecurity implementation. Instead, governance mechanisms such as leadership commitment, continuous monitoring, staff education, organizational accountability, and incident response planning determine whether legal requirements translate into effective protection of patient information.

Recent legal scholarship further expands this perspective by emphasizing the responsibilities of clinicians, healthcare institutions, and third-party service providers. The increasing adoption of cloud computing, artificial intelligence, and digital health platforms has created new legal challenges regarding data ownership, cross-organizational responsibility, and liability for cybersecurity incidents. Consequently, legal protection increasingly requires integrated governance involving healthcare providers, technology vendors, regulators, and patients.

Discussion

The present review demonstrates that medical data leakage should no longer be viewed as an isolated cybersecurity problem. Instead, the reviewed evidence indicates that healthcare data leakage represents a multidimensional governance challenge involving technological infrastructure, organizational capability, legal compliance, and patient trust. Across the reviewed studies, these dimensions repeatedly interacted to shape both the occurrence of data breaches and the effectiveness of organizational responses.

One important observation emerging from this review is the shift in healthcare cybersecurity research from a technology-centered perspective toward a governance-oriented perspective. Earlier studies predominantly emphasized technical solutions such as encryption, authentication mechanisms, blockchain, and intrusion detection systems as the primary means of protecting medical information. More recent studies, however, suggest that technological controls alone cannot adequately protect healthcare organizations from increasingly sophisticated cyber threats. Instead, cybersecurity resilience depends on how organizations integrate technology with leadership commitment, staff capability, organizational culture, and institutional governance. This finding is consistent with the sociotechnical perspective, which argues that cybersecurity failures rarely originate from technological weaknesses alone. Human behavior, organizational routines, resource allocation, and institutional policies interact with technical vulnerabilities to create conditions that enable medical data leakage. Consequently, strengthening healthcare cybersecurity requires organizational transformation rather than simply implementing additional security technologies.

A second important finding concerns the changing nature of medical data leakage itself. The reviewed evidence suggests that healthcare information is exposed through multiple pathways rather than exclusively through malicious cyberattacks. This review identified three distinct forms of medical data leakage: malicious cyber breaches, unauthorized access or disclosure, and secondary use of personal health information beyond its original purpose. Although these three pathways all result in the loss of control over sensitive medical information, they differ substantially in their underlying causes, legal consequences, and governance requirements.

This distinction extends existing literature by emphasizing that healthcare organizations should adopt differentiated prevention strategies. Cyberattacks require technical protection and incident response capabilities, whereas unauthorized disclosure often necessitates improvements in organizational governance, staff awareness, and access management. Similarly, secondary use of health information raises questions regarding informed consent, transparency, and patient autonomy that cannot be resolved solely through technical cybersecurity measures. Therefore, future healthcare governance frameworks should explicitly recognize these different pathways rather than treating all medical data leakage incidents as equivalent.

The review also demonstrates that legal compliance should not be interpreted as evidence of effective cybersecurity. Several reviewed studies indicate that healthcare organizations continue to experience substantial data breaches despite complying with regulatory requirements such as HIPAA (Tovino, 2025). This observation suggests that legal compliance represents a minimum governance requirement rather than a guarantee of effective information security. Regulations establish organizational responsibilities, reporting obligations, and accountability mechanisms, but their effectiveness depends on institutional implementation, leadership commitment, continuous monitoring, and organizational learning.

For countries currently strengthening personal data protection legislation, including Indonesia, these findings have important policy implications. The enactment of legal frameworks such as the Personal Data Protection Law and healthcare regulations should be accompanied by organizational investment in cybersecurity governance, workforce capability, and institutional resilience (Nugroho, 2021). Without corresponding organizational capacity, legislative reforms may have limited practical impact on preventing healthcare data leakage.

Another contribution emerging from this review concerns patient privacy and trust. While healthcare organizations increasingly recognize the importance of privacy protection, the reviewed evidence suggests that patients evaluate digital healthcare services not only based on security technologies but also on organizational transparency, accountability, and perceived trustworthiness. Patients are generally willing to share health information when they understand how their data will be used, who will access it, and what safeguards are implemented to prevent misuse. Conversely, uncertainty regarding secondary use, commercial exploitation, or inadequate communication significantly reduces willingness to participate in digital healthcare initiatives.

The rapid adoption of artificial intelligence, cloud computing, mobile health applications, and interconnected medical devices further complicates healthcare data governance. Unlike traditional information systems, these technologies introduce new pathways through which patient information may be collected, processed, stored, transferred, and reused. Several reviewed studies suggest that existing regulatory frameworks have not fully anticipated these technological developments, particularly regarding AI-generated outputs, third-party service providers, cross-border data processing, and algorithmic accountability. Consequently, healthcare cybersecurity research is increasingly expanding beyond conventional hospital information systems toward broader digital health ecosystems.

Overall, this review proposes that healthcare organizations should move from a compliance-oriented approach toward a resilience-oriented governance model. Such a model integrates cybersecurity technologies, organizational governance, legal protection, and patient-centered privacy management within a unified framework. Rather than treating cybersecurity, legal compliance, and patient privacy as separate organizational responsibilities, healthcare institutions should recognize these elements as mutually reinforcing dimensions of digital healthcare governance.

Based on the evidence synthesized from the fourteen included studies, the thematic framework presented in Table 2 was developed through a relational rather than purely descriptive synthesis. The framework does not simply group findings into separate categories; instead, it maps the analytical relationship between underlying vulnerabilities, pathways of medical data leakage, resulting consequences, and corresponding governance responses.

The first relationship is supported by studies demonstrating that healthcare cybersecurity risks arise from the interaction of technological, organizational, and human factors. The evidence concerning sociotechnical vulnerabilities, security mechanisms, organizational preparedness, phishing susceptibility, and security culture supports the classification of vulnerabilities into human, organizational, and technical dimensions. The second relationship links these vulnerabilities to three principal leakage pathways: malicious cyber breaches, unauthorized access or disclosure, and secondary use of health data. The third relationship connects these pathways to consequences affecting patient privacy, patient safety, institutional liability, financial loss, reputational damage, and public trust.

The final relationship concerns governance responses. The reviewed studies consistently indicate that no single intervention—whether technological, legal, or organizational—is sufficient to address all forms of medical data leakage. Technical safeguards such as encryption, authentication, access control, and intrusion detection must therefore interact with legal obligations concerning privacy, breach notification, accountability, and patient rights, while organizational governance must provide leadership, risk assessment, workforce preparedness, vendor management, incident response, transparency, and accountability.

The novelty of the framework therefore lies in its proposed causal-governance logic: vulnerabilities create conditions that enable specific leakage pathways; those pathways generate different forms of harm; and the nature of the harm determines the combination of technological, legal, organizational, and patient-centered responses required. Rather than treating cybersecurity, privacy, legal protection, and governance as separate analytical domains, Table 2 integrates them into a single explanatory model that can be further tested in future empirical research.

Table 2. Thematic Synthesis Framework of Medical Data Leakage in Healthcare

Healthcare Cybersecurity Vulnerabilities	Medical Data Leakage Pathways	Consequences	Integrated Governance Response
Human Factors	Malicious Cyber Breach	Loss of patient privacy	Cybersecurity Technology
Human error	Ransomware		Encryption
Phishing susceptibility	Hacking		Multi-factor authentication (MFA)
Low cybersecurity awareness	Malware attacks		Access control
Weak security culture			Intrusion detection systems
Organizational Factors	Unauthorized Access / Disclosure	Patient safety risks	Legal Protection
Legacy systems	Insider misuse		HIPAA
Limited cybersecurity investment	Credential misuse		GDPR
Weak governance	Improper data sharing		Personal Data Protection regulations
Inadequate incident response			Breach notification
Technical Factors	Secondary Use of Health Data	Legal liability	Healthcare Governance
IoMT vulnerabilities	AI model training	Financial losses	Leadership commitment
Cloud computing risks'AI security risks	Research use	Reputational damage	Risk assessment
Network vulnerabilities	Commercial data reuse	Loss of public trust	Vendor management
			Incident response
			Transparency
			Individual control
			Accountability

Conclusion

This systematic literature review synthesizes the current body of knowledge on medical data leakage from the perspectives of healthcare cybersecurity, patient privacy, legal protection, and organizational governance. The review demonstrates that medical data leakage is a multifaceted phenomenon that extends beyond technical cybersecurity incidents. Instead, data leakage arises from the interaction of technological vulnerabilities, human and organizational factors, regulatory implementation, and the governance of health information throughout its lifecycle.

The thematic synthesis identified four overarching themes. First, healthcare cybersecurity vulnerabilities originate not only from cyber threats such as ransomware, phishing, and legacy systems, but also from organizational weaknesses including inadequate cybersecurity investment, limited staff awareness, and insufficient governance. Second, medical data leakage occurs through multiple pathways, including malicious cyber

breaches, unauthorized access or disclosure, and secondary use of health data beyond its original purpose, each requiring different preventive and regulatory approaches. Third, legal protection remains an essential component of healthcare information security; however, compliance with regulations such as HIPAA or GDPR alone does not guarantee effective protection against data breaches. Effective implementation depends on organizational readiness, leadership commitment, continuous monitoring, and cybersecurity culture. Fourth, preventing medical data leakage requires an integrated governance approach that combines technological safeguards, legal compliance, organizational capability, and patient-centered privacy management.

From a practical perspective, healthcare organizations should move beyond compliance-oriented cybersecurity strategies and adopt a Healthcare Cyber Resilience Governance Framework. The proposed framework consists of seven measurable dimensions that can be operationalized and empirically tested in future research. First, cybersecurity control capacity should assess the implementation of technical safeguards, including encryption, multi-factor authentication, access control, network segmentation, vulnerability management, intrusion detection, backup systems, and regular security testing. Second, organizational preparedness should measure the existence and quality of cybersecurity policies, workforce training, security awareness, risk assessments, simulation exercises, and continuity planning. Third, legal and regulatory compliance should evaluate whether the healthcare organization has implemented procedures concerning lawful data processing, informed consent, purpose limitation, breach notification, documentation, and regulatory accountability. Fourth, patient privacy and individual control should assess the extent to which patients are informed about the collection, use, sharing, retention, and secondary use of their medical information, including the availability of mechanisms to exercise relevant privacy rights.

Fifth, vendor and third-party governance should evaluate contractual safeguards, cybersecurity requirements, access restrictions, data-processing agreements, audit mechanisms, and accountability for cloud providers, artificial intelligence developers, telemedicine platforms, and other external service providers. Sixth, incident response and recovery capacity should assess the existence of incident-response teams, detection and escalation procedures, recovery capabilities, communication protocols, post-incident evaluation, and mechanisms for preventing recurrence. Seventh, institutional accountability and resilience learning should evaluate leadership commitment, internal oversight, transparency, reporting culture, audit mechanisms, corrective action, and the organization's ability to convert cybersecurity incidents into institutional learning. The proposed framework can be empirically validated by developing indicators for each dimension and measuring organizational performance through a combination of documentary assessment, cybersecurity audits, staff surveys, incident-response evaluations, and patient privacy assessments. In this sense, resilience-oriented governance should not be understood merely as a normative recommendation but as a measurable institutional capacity to anticipate, prevent, detect, respond to, recover from, and learn from medical data leakage incidents.

Future research should also investigate emerging issues that remain underexplored in the current literature, including artificial intelligence governance, third-party data processing, cross-border health data transfers, Internet of Medical Things (IoMT) security,

and the implementation of personal data protection regulations in developing countries. Comparative studies examining healthcare governance across different legal systems would further enhance understanding of how regulatory environments influence the prevention and management of medical data leakage.

References

Ahmed, F. Z. O. and S. (2025). Ethical and Legal Dimensions of AI in Healthcare: A Deep Learning Perspective. *Intelligence in Healthcare Law*. https://doi.org/10.1201/9781003538462-6

Budiman, R. (2023). The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022. *Jurnal Smart Hukum (JSH)*, *2*(1). https://doi.org/10.55299/jsh.v2i1.1352

Budiono, A., Nurrizky, A. S., Fairuzzaman, F., Gulyamov, S. S., Prakoso, A. L., Yuspin, W., Farid, A. M., & Ogli, T. M. A. P. (2024). Lesson From Indonesia National Healthcare Security (BPJS Kesehatan): HIV/AIDS Patient Medical Data Protection Policies. *Malaysian Journal of Medicine and Health Sciences*, *20*, 201–208. https://doi.org/10.47836/mjmhs.20.s9.33

Chiruvella, V., & Guddati, A. K. (2021). Ethical Issues in Patient Data Ownership. *Interactive Journal of Medical Research*, *10*(2), e22269. https://doi.org/10.2196/22269

Dehghan, M., Behzadi, A., Mehrolhassani, M. H., & Ghaemi, M. M. (2026). Challenges and facilitators of electronic health record implementation: a scoping review. *International Journal of Medical Informatics*, *205*. https://doi.org/10.1016/j.ijmedinf.2025.106094

Desai, A. U., & Desai, M. (2023). A Review of the State of Cybersecurity in the Healthcare Industry and Propose Security Controls. *Mesopotamian Journal of Artificial Intelligence in Healthcare*, *2023*, 82–84. https://doi.org/10.58496/MJAIH/2023/016

Ettaloui, N., Arezki, S., & Gadi, T. (2024). An Overview of Blockchain-Based Electronic Health Record and Compliance with GDPR and HIPAA. *Lecture Notes in Networks and Systems*, *838 LNNS*, 405–412. https://doi.org/10.1007/978-3-031-48573-2_58

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. *Journal of Medical Internet Research*, *26*. https://doi.org/10.2196/46904

Ewoh, P., Vartiainen, T., & Mantere, T. (2025). Sociotechnical Cybersecurity Framework for Securing Health Care From Vulnerabilities and Cyberattacks: Scoping Review. *Journal of Medical Internet Research*, *27*. https://doi.org/10.2196/75584

Hoofnagle, C. J., Sloot, B. van der, & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information and Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Hossain, M. K., Sutanto, J., Handayani, P. W., Haryanto, A. A., Bhowmik, J., & Frings-Hessami, V. (2025). An exploratory study of electronic medical record implementation and recordkeeping culture: the case of hospitals in Indonesia. *BMC Health Services Research*, *25*(1). https://doi.org/10.1186/s12913-025-12399-0

J. Starcke, J. Spadafora, J. Spadafora, P. Spadafora, and M. T. (2025). The Effect of Data Leakage and Feature Selection on Machine Learning Performance for Early Parkinson's Disease Detection. *Bioengineering*, *12*(8). https://doi.org/10.3390/bioengineering12080845

Keith Mweebo. (2014). Security of Electronic Health Records in a Resource Limited Setting: the Case of Smart-Care Electronic Health Record in Zambia. *3rd Australian EHealth Informatics and Security Conference*. https://ro.ecu.edu.au/aeis/21/

Lee, T. F., Li, H. Z., & Hsieh, Y. P. (2021). A blockchain-based medical data preservation scheme for telecare medical information systems. *International Journal of Information Security*, *20*(4), 589–601. https://doi.org/10.1007/s10207-020-00521-8

McMullen, P. C., Howie, W. O., Philipsen, N., Bryant, V. C., Setlow, P. D., Calhoun, M., & Green, Z. D. (2014). Electronic medical records and electronic health records: Overview fornurse practitioners. *Journal for Nurse Practitioners*, *10*(9), 660–665. https://doi.org/10.1016/j.nurpra.2014.07.013

MULUKUNTLA, S. (2015). Interoperability in Electronic Medical Records: Challenges and Solutions for Seamless Healthcare Delivery. *International Journal of Medical and Health Science*, *1*(1), 31–38. https://eijmhs.com/index.php/mhs/article/view/214

Munoko, I., & others. (2023). Ethical Challenges of AI in Accounting. *Modern Accounting Review*. available: https://research-api.cbs.dk/ws/portalfiles/portal/108045502/1845662_MasterThesis_A.Benahmida_158615.pdf

Nugroho, A. A. P. and A. P. (2021). Digital Transformation in Indonesian Healthcare. *STI Policy and Management Journal*, *6*(1). https://doi.org/10.14203/stipm.2021.301

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. *Bmj*, *372*. https://doi.org/10.1136/bmj.n71

S. J. Nass and O. L. Levit, L. A. G. (2014). The Value and Importance of Health Information Privacy - Beyond the ... 2 The Value and Importance of Health Information Privacy The Value and Importance of Health Information Privacy - Beyond the ... *In Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, 1–15.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare (Switzerland)*, *8*(2). https://doi.org/10.3390/healthcare8020133

Shi, S., Haque, M. S., Parida, A., Zhang, C., Linguraru, M. G., Thomas Hou, Y., Anwar, S. M., & Lou, W. (2025). MedLeak: Multimodal Medical Data Leakage in Secure Federated Learning with Crafted Models. *Proceedings - 2025 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2025*, 245–256. https://doi.org/10.1145/3721201.3721375

Subekti, S. A. S. D. and R. (2024). Pertanggungjawaban Penyedia Sistem Rekam Medis Elektronik Dari Partner System Terhadap Kebocoran Data. *Demokrasi: Jurnal Riset Ilmu Hukum, Sosial Dan Politik*, *1*(3). https://doi.org/10.62383/demokrasi.v1i3.253

Tovino, S. A. (2025). Artificial Intelligence and the HIPAA Privacy Rule: A Primer. *Houston Journal of Health Law & Policy*, *24*(1), 77–726. https://digitalcommons.law.ou.edu/cgi/viewcontent.cgi?params=/context/fac_articles/article/1648/&path_info=Tovino_2025_Artificial_Intelligence_and_the_HIPAA_Privacy_Rule.pdf

Zakzouk, A., El-Sayed, A., & Hemdan, E. E. D. (2023). A blockchain-based electronic medical records management framework in smart healthcare infrastructure. *Multimedia Tools and Applications*, *82*(23), 35419–35437. https://doi.org/10.1007/s11042-023-15152-z

.