EDU REKHA INTERNATIONAL JOURNAL OF ARTS, LAW AND SOCIAL SCIENCE

Journal Homepage: https://edurekhapublisher.com/erijalss/

Volume- 2 Issue – 4 (July-August) 2026

ISSN: 3107-5169 (Online)

Frequency: Bimonthly

PAGES: 223-231

ARTICLE TITLE:

RECONSTRUCTION OF CRIMINAL LIABILITY FOR THE MISUSE OF ELECTRONIC MEDICAL RECORDS IN REALIZING LEGAL PROTECTION AND LEGAL CERTAINTY FOR PATIENTS

Henny Saida Flora[1*] & Maidin Gultom[2]

[1&2]Professor, Department of Law, Universitas Katolik Santo Thomas, Indonesia

ARTICLE HISTORY

RECEIVED
08-08-2026

ACCEPTED
11-08-2026

PUBLISHED
23-08-2026

Corresponding author:

Henny Saida Flora

Professor, Department of Law, Universitas Katolik Santo Thomas, Indonesia

Abstract

The development of digital health services has transformed the management, storage, and exchange of patient information through the implementation of Electronic Medical Records (EMRs). Although EMRs provide significant benefits in improving the efficiency, accuracy, and continuity of healthcare services, their use also creates potential risks of unauthorized access, disclosure, alteration, manipulation, and misuse of patient data. These circumstances raise important legal issues concerning the criminal liability of individuals or institutions responsible for the misuse of electronic medical records and the effectiveness of existing legal mechanisms in protecting patients. This study aims to analyze the legal framework governing criminal liability for the misuse of electronic medical records and to reconstruct a criminal liability model that provides stronger legal protection and legal certainty for patients.

This research employs normative juridical methods using a statutory, conceptual, and case-based approach. Legal materials are analyzed qualitatively to identify regulatory gaps, inconsistencies, and weaknesses in the implementation of criminal liability relating to electronic medical records. The findings indicate that the existing legal framework provides several forms of protection for the confidentiality and security of medical information; however, challenges remain concerning the determination of responsible parties, unauthorized access, data disclosure, manipulation, and the application of criminal sanctions in the digital healthcare environment. Therefore, a reconstruction of criminal liability is necessary by establishing clear standards concerning prohibited conduct, the subjects who may be held criminally liable, institutional responsibility, forms of sanctions, and mechanisms for protecting and restoring patients' rights. Such reconstruction is expected to strengthen legal protection, ensure legal certainty, and establish accountability in the management of electronic medical records.

Keywords: Electronic Medical Records; Criminal Liability; Misuse of Medical Records; Legal Protection; Legal Certainty; Patients' Rights; Data Privacy.

INTRODUCTION

The rapid development of information technology has fundamentally transformed the healthcare sector, particularly in the management, storage, processing, and exchange of patient information. One of the most significant developments is the implementation of Electronic Medical Records (EMRs), which enables healthcare providers to digitally document, manage, and access patients' medical information. The use of EMRs provides substantial benefits, including improving the efficiency and accuracy of healthcare services, facilitating continuity of care, reducing administrative burdens, and supporting healthcare professionals in making clinical decisions. However, the digitalization of medical records also creates new legal challenges, particularly concerning confidentiality, data security, unauthorized access, disclosure, alteration, manipulation, and misuse of patients' medical information.

Medical records contain highly sensitive information concerning a patient's identity, medical history, diagnosis, treatment, health condition, and other personal information. Therefore, the management of medical records cannot merely be regarded as an administrative component of healthcare services. It constitutes an important dimension of the protection of patients' privacy and personal rights. Unauthorized access to or disclosure of medical information may cause not only material losses but also psychological, social, professional, and reputational harm to patients. Consequently, the misuse of electronic medical records raises fundamental questions regarding the extent to which criminal law can provide effective protection for patients while simultaneously ensuring legal certainty for healthcare professionals and healthcare institutions.

In the Indonesian legal system, the protection of medical information is regulated through several legal instruments. (Fuady, M. 2013). The legal framework governing healthcare recognizes the importance of medical records and the confidentiality of patient information, while the development of electronic health services has created an increasing intersection between health law, personal data protection law, electronic information law, and criminal law. In particular, health data constitutes sensitive personal information that requires a higher level of protection. The existence of various legal regimes demonstrates the importance of an integrated legal framework capable of responding to violations involving electronic medical records. (Ratman, H. D, 2018)

Nevertheless, the existence of legal provisions does not automatically guarantee effective protection in practice. The misuse of electronic medical records may take various forms, including accessing patient information without authorization, disclosing medical information to unauthorized persons, using patient data for purposes beyond the original purpose of collection, altering or manipulating electronic medical records, transferring data unlawfully, and exploiting medical information for personal or commercial interests. These forms of misconduct raise complex questions concerning the determination of the responsible party, the elements of criminal liability, the applicable sanctions, and the distinction between criminal offenses, administrative violations, professional misconduct, and civil liability. Dady, R. D, 2026).

The issue becomes more complicated when electronic medical records are managed within healthcare institutions involving multiple actors, such as physicians, nurses, administrative personnel, hospital management, information technology personnel, and third-party electronic system providers. When a security breach or misuse of medical records occurs, determining the individual responsible may be difficult. The misconduct may result from intentional actions, negligence, inadequate security systems, unauthorized access by employees, or institutional failures in implementing data protection mechanisms. Consequently, the legal framework must clearly establish the scope of individual and institutional criminal liability.

From the perspective of criminal law, the formulation of liability must remain consistent with fundamental principles, particularly the principle of legality and the principle of culpability. Criminal liability cannot be imposed merely because a person is associated with the management of electronic medical records. It must be established that the relevant person committed a legally prohibited act with the required form of fault. At the same time, criminal law must respond effectively to intentional misuse and serious negligence that compromises the confidentiality and security of patients' medical information. This creates a need to establish clear boundaries concerning prohibited conduct, responsible subjects, forms of culpability, and applicable criminal sanctions.

Another significant challenge concerns the evidentiary aspects of electronic medical record misuse. Unlike conventional physical documents, electronic records can be accessed remotely, modified digitally, transferred rapidly, or deleted without leaving easily identifiable physical traces. The identification of perpetrators may therefore depend upon electronic evidence such as access logs, audit trails, authentication records, system metadata, and other digital traces. Law enforcement authorities must possess adequate technological and legal capabilities to identify, preserve, examine, and present such evidence in criminal proceedings. Weaknesses in digital evidence management may undermine the effectiveness of criminal law enforcement and ultimately reduce the protection available to patients.

Patients also occupy a relatively vulnerable position in relation to the management of their medical information. Most patients do not have sufficient knowledge concerning how their medical data is stored, who may access it, how long it is retained, or what security measures are implemented by healthcare providers. This information asymmetry may create an unequal relationship between patients and healthcare institutions or electronic system operators. When medical information is misused, patients may face consequences extending beyond financial loss, including loss of privacy, emotional distress, discrimination, reputational damage, and social consequences. Accordingly, legal protection should not be limited to imposing sanctions on perpetrators but should also provide effective mechanisms for prevention, complaint handling, investigation, recovery, and compensation for affected patients.

The principle of legal certainty is equally important in addressing the misuse of electronic medical records. Overlapping legal provisions may potentially create uncertainty regarding which legal regime should be applied, which institution has authority to investigate, and which party should bear responsibility for a particular violation. Therefore, a coherent legal framework is necessary to harmonize health law, personal data protection law, electronic information law, and criminal law. Such harmonization should ensure that patients receive effective protection without creating excessive criminalization of healthcare professionals who legitimately access and process medical information in the performance of their professional duties.

In this context, the reconstruction of criminal liability becomes necessary. Reconstruction should not merely focus on increasing criminal sanctions but should seek to establish a comprehensive model of accountability based on the nature of electronic medical records and the risks associated with their misuse. Such

reconstruction should clarify the categories of prohibited conduct, the subjects who may be held criminally liable, the distinction between intentional and negligent conduct, the potential liability of healthcare institutions and electronic system providers, evidentiary mechanisms, and the rights of patients as victims.

The reconstruction of criminal liability should ultimately seek to achieve a balance between several competing interests: the protection of patients' privacy and personal data, the legitimate interests of healthcare providers, the security and efficiency of digital healthcare systems, and the interests of law enforcement. Criminal law should provide a strong deterrent against intentional and serious misuse of electronic medical records while maintaining proportionality, fairness, and legal certainty for healthcare professionals and institutions.

Based on these considerations, this study focuses on the reconstruction of criminal liability for the misuse of electronic medical records in realizing legal protection and legal certainty for patients. The study examines the existing legal framework governing the misuse of electronic medical records, identifies regulatory and implementation gaps in criminal liability, and formulates a more comprehensive model of criminal accountability. The proposed reconstruction is expected to strengthen the protection of patients' rights, clarify the responsibilities of relevant actors, enhance the effectiveness of law enforcement, and establish a legal framework that is responsive to the continuing digital transformation of healthcare services. (Triwibowo, C, 2012).

METHOD

This study employs a normative juridical research method, which focuses on examining legal norms, principles, doctrines, and regulations governing criminal liability for the misuse of electronic medical records. This method is appropriate because the research primarily seeks to analyze the existing legal framework and reconstruct the concept of criminal liability in order to strengthen legal protection and legal certainty for patients.

The research uses a statutory approach, conceptual approach, and case approach. The statutory approach is employed to examine relevant laws and regulations concerning healthcare, medical records, personal data protection, electronic information, criminal liability, and patients' rights. The conceptual approach is used to analyze fundamental legal concepts, including criminal liability, unlawful acts, confidentiality of medical information, electronic medical records, legal protection, legal certainty, and institutional responsibility. The case approach is used to examine relevant judicial decisions and legal disputes concerning the misuse, disclosure, unauthorized access, or manipulation of medical information in order to identify problems in the application of existing legal norms. (Soekanto, S., & Mamudji, S. 2015).

The legal materials consist of primary, secondary, and tertiary legal materials. Primary legal materials include legislation, regulations, and relevant court decisions. Secondary legal materials consist of legal textbooks, scholarly articles, academic journals, research reports, and legal doctrines relevant to criminal law, health law, personal data protection, and electronic information. Tertiary legal materials include legal dictionaries, encyclopedias, and other reference materials that support the interpretation of legal concepts. (Rizkia, N. D., & Fardiansyah, H. 2023).

The collection of legal materials is conducted through library research and document analysis. Relevant legal materials are identified, classified, and systematically examined based on their relevance to the research objectives. The collected materials are subsequently analyzed using a qualitative juridical analysis. This analysis is conducted by interpreting legal norms, comparing relevant regulatory provisions, identifying inconsistencies and regulatory gaps, and examining their implications for the protection of patients' rights.

The analysis is further directed toward identifying weaknesses in the existing model of criminal liability, particularly concerning the determination of responsible subjects, forms of unlawful conduct, standards of culpability, institutional liability, criminal sanctions, and evidentiary mechanisms. Based on these findings, the study develops a reconstructive legal analysis to formulate a more comprehensive model of criminal liability for the misuse of electronic medical records.

The reconstruction is formulated based on the principles of legality, culpability, proportionality, confidentiality, accountability, legal protection, and legal certainty. The final analysis is expected to produce a normative model that balances the protection of patients' rights with the legitimate interests and legal protection of healthcare professionals, healthcare institutions, and electronic health system operators.

LITERATURE REVIEW

A. The Concept and Development of Electronic Medical Records

The development of information technology has significantly transformed the healthcare sector, particularly in the management of patient information. One of the most important manifestations of this transformation is the transition from conventional paper-based medical records to Electronic Medical Records (EMRs). Electronic medical records represent a digital form of patient health information that is systematically created, stored, managed, and accessed through an electronic information system. This transformation is not merely a change in the medium used to record medical information but also represents a fundamental change in the way healthcare information is generated, processed, exchanged, and protected.

Conceptually, an electronic medical record contains various categories of information relating to a patient, including personal identity, medical history, clinical findings, diagnosis, treatment, medication, laboratory results, medical procedures, and other information generated during the provision of healthcare services. The digital format enables healthcare professionals to access relevant information more efficiently and supports the continuity and quality of healthcare services. EMRs can also facilitate communication among healthcare professionals and improve the availability of accurate information for clinical decision-making.

From a legal perspective, however, an electronic medical record cannot be viewed merely as a technological instrument or an administrative document. It constitutes a legal document containing information that is closely related to the rights and interests of patients. The information contained in an EMR is inherently sensitive because it may reveal an individual's physical and psychological condition, medical history, treatment, and other personal circumstances. Consequently, the management of EMRs must be accompanied by legal safeguards concerning confidentiality, integrity, authenticity, availability, and security of information.

The development of EMRs has also changed the relationship between patients, healthcare professionals, healthcare facilities, and information technology providers. In a conventional paper-based system, access to medical records was generally limited by physical

control over the documents. In contrast, electronic systems enable information to be accessed simultaneously or remotely by authorized users. This characteristic provides substantial benefits but also increases the risk of unauthorized access, data leakage, alteration, duplication, and dissemination of medical information. The wider the network through which medical information is processed, the greater the potential vulnerability to misuse.

The digitalization of medical records also creates new forms of legal risk. Unauthorized access may occur when an individual obtains access credentials belonging to another person or exploits weaknesses in an information system. Medical information may also be disclosed intentionally or negligently to persons who have no legitimate interest in receiving such information. In addition, electronic records may be altered or manipulated in ways that are difficult to detect without an adequate audit trail and security mechanism. These circumstances demonstrate that the development of EMRs must be accompanied by a corresponding development of legal standards governing access, processing, storage, transfer, and disclosure of medical information.

In Indonesia, the development of electronic medical records forms part of the broader transformation of the national healthcare system toward digital health services. The legal framework recognizes medical records as an essential component of healthcare administration and professional practice. The development of electronic systems has consequently required adjustments to the legal framework concerning the creation, storage, confidentiality, access, and management of medical records. The regulation of EMRs must also be understood in conjunction with the legal framework concerning personal data protection and electronic information. (Punia, I. G. E. A. A. 2024)

The legal significance of EMRs becomes increasingly important because the information contained therein may serve multiple purposes. In addition to supporting diagnosis and treatment, medical records may be used for healthcare administration, quality control, research, education, insurance, health financing, and legal proceedings, subject to applicable legal requirements. The broader the functions of EMRs, the greater the need to establish clear boundaries concerning who may access the information, for what purpose, and under what circumstances disclosure is legally justified.

Another important characteristic of EMRs is the requirement of data integrity and authenticity. Medical information must accurately reflect the healthcare services provided to the patient. Unauthorized modification or manipulation of medical records may affect subsequent medical decisions and may potentially endanger patient safety. Therefore, an effective electronic medical record system should incorporate mechanisms such as authentication, access control, audit trails, encryption, and systematic monitoring to ensure that every access or modification can be identified and verified.

From a criminal law perspective, the development of EMRs creates a new area of concern regarding the determination of unlawful conduct and criminal responsibility. Not every violation involving an electronic medical record should automatically be classified as a criminal offense. There must be a clear distinction between legitimate access, professional use, administrative error, negligence, and intentional misuse. Criminal liability should therefore be based on clear statutory provisions and the existence of the requisite elements of a criminal offense and culpability.

The development of EMRs thus presents a dual character. On the one hand, digitalization improves the efficiency, accessibility, accuracy, and continuity of healthcare services. On the other hand, it increases the complexity of protecting sensitive medical information from unauthorized access and misuse. This duality demonstrates that technological development must be accompanied by legal development. The law must not only regulate the use of technology but also anticipate new forms of harm arising from digital healthcare systems.

Accordingly, the development of electronic medical records requires a comprehensive legal framework that integrates health law, criminal law, personal data protection law, and electronic information law. Such integration is essential to establish clear standards of responsibility for every party involved in the management of EMRs. At the same time, it must ensure that patients receive effective protection while healthcare professionals and healthcare institutions obtain sufficient legal certainty when performing legitimate medical and administrative functions.

Ultimately, the concept and development of electronic medical records demonstrate that the digital transformation of healthcare is not merely a technological issue but also a legal and human rights issue. The protection of patients' medical information must therefore become an integral component of the digital healthcare system. The development of EMRs should be accompanied by mechanisms capable of preventing misuse, identifying violations, establishing accountability, and providing effective remedies for patients whose rights have been infringed. This framework provides the conceptual foundation for examining the reconstruction of criminal liability for the misuse of electronic medical records in order to achieve stronger legal protection and legal certainty for patients.

B. Legal Protection of Patients in the Management of Electronic Medical Records

The legal protection of patients in the management of Electronic Medical Records (EMRs) is an essential element of modern healthcare governance. The digitalization of medical records provides significant benefits for healthcare services by facilitating the storage, retrieval, processing, and exchange of patient information. However, because EMRs contain sensitive personal and health information, their management also creates significant risks concerning privacy, confidentiality, data security, and unauthorized use. Therefore, the development of electronic healthcare systems must be accompanied by adequate legal protection to ensure that patients' rights are effectively safeguarded. Magdalena, (M., Sarwo, Y. B., & Wibowo, D. B. 2024).

From a legal perspective, patients have the right to have their medical information kept confidential and protected from unauthorized access or disclosure. Medical information includes personal identity, medical history, diagnosis, treatment, medication, laboratory results, and other information concerning the patient's health condition. Such information is highly sensitive because its disclosure may cause various forms of harm, including psychological distress, social stigma, discrimination, reputational damage, and economic loss. Consequently, healthcare providers and other parties involved in managing EMRs must maintain the confidentiality and security of patient information.

Legal protection may generally be divided into preventive and repressive protection**.** Preventive protection aims to prevent violations before they occur. It includes clear rules concerning access rights, authentication mechanisms, confidentiality obligations, data encryption, information security standards, audit trails, employee authorization, and procedures for the lawful disclosure of medical information. Healthcare institutions should ensure that only individuals with legitimate professional or legal purposes are permitted to access particular categories of patient

information. The principle of limited access is particularly important because not every person working within a healthcare institution should have unrestricted access to all patient records.

Preventive protection also requires healthcare institutions to establish internal policies governing the collection, storage, use, transfer, retention, and destruction of electronic medical records. Employees and healthcare professionals who have access to EMRs should receive adequate training concerning confidentiality, cybersecurity, professional ethics, and personal data protection. In addition, institutions should conduct regular security assessments to identify potential vulnerabilities in their electronic medical record systems. These preventive mechanisms are essential because technological security and legal protection must operate together. A sophisticated technological system without clear legal responsibility may still create significant risks for patients.

Repressive legal protection becomes relevant when a violation of patients' rights has already occurred. Misuse of EMRs may take various forms, including unauthorized access, unlawful disclosure, alteration or manipulation of medical information, illegal transfer of patient data, unauthorized copying, and the use of medical information for purposes unrelated to healthcare services. Depending on the nature and severity of the conduct, such violations may result in professional, administrative, civil, or criminal liability.

The determination of liability is particularly important in cases involving electronic medical records because several parties may participate in the management of patient information. Physicians, nurses, administrative personnel, hospital management, information technology personnel, and third-party electronic system providers may have different levels of access and responsibility. Therefore, the legal framework must clearly determine which person or institution is responsible for a particular violation. Individual liability should be based on the person's actual conduct and level of fault, while institutional liability may arise when the violation results from inadequate organizational controls, failure to implement security measures, or negligent management of electronic systems. (Shah, S. M., & Khan, R. A, 2020)

Patient protection is also closely related to the principle of data minimization and purpose limitation. Medical information should only be collected and processed for legitimate and clearly defined purposes. The use of patient information for unrelated purposes without a valid legal basis may constitute a violation of the patient's rights. This principle is particularly significant in the digital healthcare environment because electronic information can easily be duplicated, transferred, analyzed, or shared with other parties.

Another important aspect is the patient's right to know how his or her medical information is managed. Patients should receive adequate information concerning the collection and use of their data, the purposes for which the information is processed, and the parties who may lawfully access it. Transparency is essential for establishing trust between patients and healthcare providers. At the same time, transparency must be balanced with legitimate healthcare needs and applicable legal exceptions, particularly where disclosure is required by law or necessary for specific public interests.

In the Indonesian legal context, the protection of patient information in EMRs is supported by several interconnected legal regimes, including health law, personal data protection law, electronic information law, and professional regulations governing healthcare providers. The existence of multiple legal instruments demonstrates that the protection of electronic medical records cannot be addressed through a single legal perspective. Instead, an integrated approach is necessary to harmonize the protection of medical confidentiality, personal data, electronic information, and patients' rights. (Siregar, R. A., & Sinaga, H. S. R. 2025).

The protection of patients must also extend to situations involving data breaches. When an unauthorized disclosure or security incident occurs, healthcare institutions should have a clear mechanism for identifying the breach, limiting its impact, notifying the relevant parties where legally required, investigating its cause, and taking corrective measures. Patients who suffer harm should have access to effective complaint mechanisms and appropriate legal remedies. Such remedies may include restoration of rights, compensation, or other forms of legal redress depending on the applicable legal framework. (Prasetyo, T. 2016)

A significant challenge in protecting EMRs is the difficulty of establishing whether unauthorized access or manipulation was committed intentionally or resulted from negligence. Criminal liability should therefore not be imposed automatically whenever a security incident occurs. The principles of **legality, culpability, proportionality, and due process** must remain the basis for determining criminal responsibility. Intentional misuse, deliberate disclosure, and fraudulent manipulation should be distinguished from technical failures, administrative errors, or unavoidable system vulnerabilities. This distinction is necessary to ensure fairness while maintaining effective protection for patients.

Furthermore, effective legal protection requires strong institutional supervision. Healthcare institutions should establish internal monitoring mechanisms capable of detecting unusual access patterns, unauthorized downloads, improper data transfers, and other suspicious activities. The existence of audit trails and access logs is particularly important because they can help identify who accessed a patient's information, when the access occurred, and what actions were performed. These mechanisms not only prevent misuse but can also support the investigation and prosecution of violations when necessary.

Ultimately, legal protection of patients in the management of Electronic Medical Records should be understood as a comprehensive system involving prevention, confidentiality, data security, accountability, enforcement, and recovery**.** The objective is not merely to prevent unauthorized disclosure but also to ensure that patients have effective legal remedies when their rights are violated. A strong legal framework must therefore provide clear standards regarding the duties of healthcare providers, the responsibilities of electronic system operators, the rights of patients, the forms of prohibited conduct, and the consequences of violations.

Accordingly, the protection of patients in the digital healthcare environment must develop alongside technological advancement. The law should be sufficiently flexible to respond to emerging forms of electronic medical record misuse while maintaining clear and predictable standards of criminal liability. Such an approach is essential for achieving a balance between the efficient use of medical information for healthcare purposes and the protection of patients' privacy, dignity, and personal rights. Effective legal protection ultimately strengthens public trust in digital healthcare services and provides the foundation for **legal certainty, accountability, and respect for patients' rights.**

C. Criminal Liability for the Misuse of Electronic Medical Records

The increasing use of Electronic Medical Records (EMRs) in healthcare services has created significant legal challenges concerning the protection of confidential patient information and the

determination of criminal liability for its misuse. EMRs contain highly sensitive personal and health information, including patients' identities, medical histories, diagnoses, treatment records, laboratory results, and other information generated during healthcare services. The unauthorized access, disclosure, alteration, manipulation, or exploitation of such information may violate patients' fundamental rights and, under certain circumstances, constitute a criminal offense. Therefore, the regulation of criminal liability for the misuse of EMRs must provide a clear balance between the protection of patients and the legitimate interests of healthcare professionals and institutions.

Criminal liability is fundamentally concerned with determining whether a person who commits an unlawful act can be held responsible and subjected to criminal sanctions. Criminal liability generally requires the existence of a prohibited act, unlawfulness, culpability, and the absence of circumstances that legally justify or excuse the conduct. In the context of electronic medical records, criminal liability cannot be imposed merely because a person has access to patient information or because a security breach occurs within a healthcare institution. It must be established that the relevant individual or entity committed a legally prohibited act and possessed the form of fault required by the applicable criminal provision.

The principle of legality constitutes a fundamental limitation on criminal liability. A person may only be punished when the conduct has been clearly defined as a criminal offense by law. This principle is particularly important in the digital healthcare environment because technological development frequently creates new forms of misconduct before the legal system has specifically addressed them. Consequently, criminal liability for EMR misuse must be based on sufficiently clear and predictable legal provisions.

The principle of culpability is equally important. Criminal responsibility should generally be based on intentional conduct or negligence where the applicable law recognizes negligence as a basis for liability. Therefore, intentional disclosure of confidential medical information should be distinguished from accidental disclosure caused by an administrative error or technical failure. This distinction is necessary to ensure that criminal law is applied proportionately and fairly.

The misuse of EMRs may occur in various forms.

First, unauthorized access occurs when an individual accesses a patient's medical record without having legitimate professional, administrative, or legal authority to do so. For example, an employee may access the medical records of a patient out of personal curiosity or for purposes unrelated to healthcare services.

Second, unauthorized disclosure occurs when confidential medical information is intentionally or negligently communicated, transmitted, published, or otherwise made available to unauthorized persons. Disclosure may occur through direct communication, electronic transmission, social media, messaging applications, or other digital platforms.

Third, alteration or manipulation of medical records constitutes another serious form of misuse. The integrity of medical information is essential because inaccurate records may influence subsequent medical decisions and potentially endanger patient safety. Deliberate modification of an EMR to conceal medical negligence, falsify treatment information, or create a misleading record may therefore have significant legal consequences.

Fourth, medical information may be copied, transferred, or commercially exploited without a legitimate legal basis. Patient data may be attractive for commercial purposes, research, marketing, insurance, or other activities. The use of such information beyond its legitimate purpose raises questions concerning the legality of data processing and the responsibility of persons who facilitate or benefit from the misuse.

Healthcare professionals are among the principal actors who have legitimate access to EMRs. Physicians, nurses, pharmacists, and other healthcare professionals require access to medical information to provide appropriate healthcare services. However, legitimate professional access does not provide unrestricted authority to use or disclose all information contained in an EMR. (Sudjana, S. (2017).

Healthcare professionals may be subject to criminal liability when they intentionally disclose confidential patient information without legal justification, manipulate medical records, access records for illegitimate purposes, or otherwise misuse patient information in violation of applicable law. Professional status should not constitute immunity from criminal responsibility. At the same time, criminal liability should not be imposed merely because a healthcare professional makes an unintentional administrative mistake.

The determination of criminal responsibility must therefore consider the person's actual authority, purpose of access, professional duties, knowledge, intention, and degree of fault. This approach is important to maintain a balance between protecting patients and ensuring that healthcare professionals can perform their legitimate professional duties without excessive fear of criminal prosecution.

The management of EMRs is frequently conducted within hospitals, clinics, laboratories, and other healthcare institutions. Consequently, misuse of patient information may arise not only from the conduct of individual employees but also from institutional failures. A healthcare institution may potentially bear legal responsibility when it fails to implement adequate security measures, permits unauthorized access, neglects employee authorization procedures, or fails to establish appropriate mechanisms for monitoring and controlling access to patient data. Institutional responsibility becomes particularly important when a data breach results from systemic weaknesses rather than the isolated conduct of an individual employee. The concept of institutional or corporate criminal liability must therefore be considered in determining accountability for serious violations involving electronic medical records. However, such liability must be formulated carefully to avoid imposing criminal responsibility automatically on an institution for every misconduct committed by an employee. There must be a legally recognized basis connecting the institutional failure, management decision, or organizational negligence to the criminal offense.

The digital management of medical records often involves third-party technology providers that develop, operate, maintain, or host electronic health systems. These providers may have significant technical access to medical information and may therefore become important actors in the protection of patient data. Criminal liability may arise when a system provider intentionally accesses, discloses, transfers, manipulates, or exploits medical information without authorization. Liability may also become relevant where the provider deliberately disregards legally required security standards or facilitates unauthorized access.

However, technical system failure should not automatically be equated with criminal conduct. A distinction must be made between ordinary technological failure, unavoidable cybersecurity incidents,

negligence, and intentional misconduct. The applicable legal framework should establish clear standards concerning the duties and responsibilities of electronic system providers. Criminal sanctions for EMR misuse must be proportionate to the seriousness of the conduct and the harm caused. Factors such as the nature of the information disclosed, the number of affected patients, the intention of the perpetrator, the extent of the dissemination, the economic benefit obtained, and the consequences suffered by the victim may be relevant in determining the appropriate sanction.

Not every violation should necessarily result in imprisonment. Depending on the circumstances, administrative sanctions, professional sanctions, civil remedies, or other measures may be more appropriate. Criminal law should operate as a strong instrument against serious and intentional violations while avoiding unnecessary criminalization of minor administrative errors.

One of the major challenges in criminal prosecution is proving who accessed, modified, or disclosed electronic medical information. Unlike physical records, electronic information may be accessed remotely and modified without obvious physical evidence. Digital evidence such as access logs, audit trails, authentication records, metadata, system records, electronic communications, and device information may therefore become crucial in establishing criminal responsibility. The reliability and integrity of such evidence must be preserved throughout the investigation and judicial process.

Digital evidence such as access logs, audit trails, authentication records, metadata, system records, electronic communications, and device information may therefore become crucial in establishing criminal responsibility. The reliability and integrity of such evidence must be preserved throughout the investigation and judicial process. Healthcare institutions should maintain adequate audit trails capable of recording access to patient information. Such records can assist law enforcement authorities in determining the identity of the user, the time of access, the information accessed, and the actions performed within the system. Proper digital evidence management consequently serves both patient protection and due process.

Criminal liability for EMR misuse should ultimately serve the broader objective of protecting patients' rights. Criminal law provides a deterrent function by communicating that serious violations of medical confidentiality and data security will have legal consequences. However, punishment alone is insufficient.

An effective legal framework should also provide mechanisms for victims to obtain remedies, including restoration of rights, compensation, and other forms of recovery where appropriate. Patients should have accessible mechanisms for reporting violations and obtaining information about the handling of their complaints.

Therefore, criminal law should operate as part of a broader legal protection system involving preventive regulation, institutional supervision, professional ethics, administrative sanctions, civil remedies, and criminal enforcement. Therefore, criminal law should operate as part of a broader legal protection system involving preventive regulation, institutional supervision, professional ethics, administrative sanctions, civil remedies, and criminal enforcement.

The complexity of electronic medical record management demonstrates the need to reconstruct the existing model of criminal liability. Such reconstruction is necessary because conventional approaches to medical confidentiality and document misuse may not adequately address the characteristics of digital information systems. The reconstructed framework should clearly identify the prohibited forms of conduct, the persons or entities that may be held responsible, the applicable standards of intent and negligence, the relationship between individual and institutional liability, and the appropriate sanctions. It should also establish clear rules concerning digital evidence and mechanisms for protecting and compensating patients who suffer harm.

The reconstruction should be based on several fundamental principles, including legality, culpability, proportionality, accountability, confidentiality, data security, victim protection, and legal certainty. These principles are necessary to ensure that criminal law remains effective without becoming excessive or unpredictable. Ultimately, the objective of criminal liability for the misuse of Electronic Medical Records is not merely to punish offenders but to establish a secure and accountable healthcare information environment. A clear and coherent framework of criminal responsibility can strengthen public confidence in digital healthcare services, protect the confidentiality and integrity of patient information, and provide legal certainty for healthcare professionals, healthcare institutions, and electronic system providers. Such a framework constitutes an essential foundation for reconstructing criminal liability in accordance with the demands of technological development and the protection of patients' rights.

D. Reconstruction of Criminal Liability for the Misuse of Electronic Medical Records

The rapid development of digital healthcare has fundamentally changed the way medical information is created, stored, processed, and exchanged. Electronic Medical Records (EMRs) provide substantial benefits for healthcare services, but they also create new forms of legal risk, particularly unauthorized access, disclosure, alteration, manipulation, and exploitation of patient information. These developments demonstrate that the traditional legal framework governing medical confidentiality and professional responsibility requires continuous adjustment to ensure effective protection of patients in the digital environment. Therefore, the reconstruction of criminal liability for the misuse of EMRs is necessary to establish a legal framework that is clear, comprehensive, proportional, and responsive to technological developments.

The concept of reconstruction in this context does not merely mean increasing criminal sanctions. It refers to the restructuring and refinement of the existing legal framework concerning the definition of prohibited conduct, the determination of responsible subjects, the standards of culpability, the forms of institutional responsibility, the evidentiary framework, and the legal remedies available to patients. The objective is to eliminate regulatory gaps and overlapping provisions while establishing a coherent system of criminal accountability.

The first aspect requiring reconstruction is the formulation of prohibited conduct involving EMRs. Existing legal provisions should clearly distinguish between legitimate access and unlawful access. Healthcare professionals may access patient information when such access is necessary for legitimate healthcare purposes. However, access undertaken out of personal curiosity, commercial interests, personal relationships, or other unauthorized purposes should be clearly identified as unlawful.

The reconstructed framework should expressly regulate several forms of prohibited conduct, including unauthorized access, unlawful disclosure, unauthorized copying or transfer, manipulation or alteration of medical information, destruction of electronic records, and exploitation of patient information for personal or commercial gain. Clear formulation is necessary to satisfy the principle of legality and criminally liable. The management of EMRs involves multiple actors, including physicians, nurses,

administrative personnel, hospital management, information technology personnel, and third-party electronic system providers.

Criminal liability should therefore not be limited to healthcare professionals. A person who intentionally accesses or misuses medical information without authorization should be subject to liability regardless of his or her professional position. At the same time, the law should distinguish between individual responsibility and institutional responsibility based on the actual role, authority, conduct, and degree of fault of each party. The digital management of medical records creates the possibility that violations may result from institutional failures rather than solely from individual misconduct. For example, a healthcare institution may fail to implement adequate access controls, employee authentication, cybersecurity measures, audit mechanisms, or internal monitoring procedures. Therefore, reconstruction should provide clearer standards for institutional and corporate criminal liability. A healthcare institution or electronic system provider should potentially be held accountable where a criminal offense results from organizational policies, management decisions, systematic negligence, or a failure to implement legally required security measures.

However, institutional liability must be based on a legally established connection between the organization's conduct or failure and the criminal offense. The mere fact that an employee committed an offense should not automatically result in criminal liability for the institution. Criminal liability must also be reconstructed by establishing clear standards concerning intentional conduct and negligence. Intentional misuse occurs when a person knowingly and deliberately accesses, discloses, manipulates, or exploits patient information without legal authorization. Such conduct represents a serious violation of the patient's rights and should attract appropriate criminal sanctions. Negligence requires a different legal assessment. A healthcare professional or institution may fail to implement appropriate security procedures or may negligently allow unauthorized access to patient information. However, negligence should only constitute a criminal offense where the applicable legislation expressly provides for criminal liability based on negligence. This distinction is essential to ensure proportionality and to prevent the criminal law from being applied excessively to ordinary technical failures or minor administrative mistakes.

The reconstruction of criminal liability should also address the proportionality of sanctions. Criminal sanctions should reflect the seriousness of the violation, the intention of the perpetrator, the extent of the disclosure, the number of affected patients, the nature of the information involved, the economic benefit obtained, and the harm suffered by the victim.

For serious and intentional misuse, criminal sanctions may serve a deterrent and retributive function. However, less serious violations caused by negligence or administrative failure may be addressed through administrative, professional, or civil mechanisms where criminal liability is not justified. A proportional sanctioning system is necessary to protect patients while ensuring fairness and legal certainty for healthcare professionals and institutions.

One of the most important elements of reconstruction concerns the evidentiary framework. EMR misuse frequently occurs in digital environments where traditional forms of evidence may be insufficient. Therefore, the legal framework should recognize the importance of electronic evidence such as access logs, audit trails, authentication records, metadata, electronic communications, and system records.

Healthcare institutions should be required to maintain reliable audit trails that can demonstrate who accessed a medical record, when the access occurred, what information was accessed, and whether the information was altered or transferred. Such records are important not only for cybersecurity but also for criminal investigations and judicial proceedings. The reconstruction should also establish standards for the preservation, authentication, examination, and presentation of electronic evidence to ensure its reliability and integrity. Criminal law should operate together with preventive and supervisory mechanisms. Healthcare institutions should be required to establish clear policies regarding access authorization, password management, data encryption, employee training, cybersecurity, audit trails, incident reporting, and regular security assessments. Supervision should also involve relevant government institutions and professional bodies. Effective oversight can identify vulnerabilities before they develop into serious violations and can reduce the need for criminal enforcement. Accordingly, the reconstructed model should adopt an integrated approach consisting of prevention, detection, accountability, enforcement, and recovery.

The ultimate objective of reconstructing criminal liability is to establish a balance between the protection of patients and the legal certainty of healthcare professionals and institutions. The law must provide sufficient protection against unauthorized access and misuse while allowing legitimate medical professionals to access information necessary for patient care. The reconstructed model should therefore be based on the principles of legality, culpability, proportionality, accountability, confidentiality, privacy, victim protection, and legal certainty. These principles provide the normative foundation for determining when the misuse of EMRs constitutes a criminal offense and who should be held responsible. The reconstruction may be conceptually formulated through the following framework: Clear Prohibited Conduct → Clear Responsible Subjects → Clear Standards of Culpability → Individual and Institutional Accountability → Reliable Digital Evidence → Proportionate Sanctions → Effective Patient Remedies. This framework demonstrates that criminal liability should be designed as an integrated system rather than merely as a mechanism for imposing punishment. Each component must function coherently to ensure that violations involving electronic medical records can be effectively prevented, investigated, prosecuted, and remedied.

Ultimately, the reconstruction of criminal liability for the misuse of Electronic Medical Records should respond to the realities of digital healthcare while maintaining the fundamental principles of criminal law. The law must provide stronger protection for the confidentiality, integrity, and security of patient information, while ensuring that criminal liability is imposed only on persons or entities whose conduct satisfies the legally established requirements. Through such reconstruction, the legal system can strengthen patient protection, improve accountability within healthcare institutions, and provide greater legal certainty for all parties involved in the management of electronic medical records.

CONCLUSION

The misuse of Electronic Medical Records (EMRs) represents a significant legal challenge in the digital transformation of healthcare services. EMRs contain sensitive personal and health information that requires strong protection against unauthorized access, disclosure, alteration, manipulation, and other forms of misuse. Although the existing legal framework provides a basis for protecting patients' medical information, the complexity of digital healthcare demonstrates the need for a more integrated and comprehensive model of criminal liability.

The reconstruction of criminal liability should begin with a clear formulation of prohibited conduct and the determination of the subjects who may be held responsible. Criminal liability must be based on the principles of legality and culpability, with a clear distinction between intentional misconduct, negligence, administrative violations, and technical failures. Responsibility should not only be considered at the individual level but should also address institutional or corporate responsibility where misuse results from organizational policies, inadequate supervision, or failure to implement appropriate security measures. Furthermore, effective enforcement requires reliable mechanisms for obtaining and verifying digital evidence, including access logs, audit trails, authentication records, metadata, and other electronic evidence. Criminal sanctions must be imposed proportionately according to the seriousness of the offense, the degree of culpability, and the harm suffered by patients. Criminal law should therefore function as part of an integrated system of preventive, administrative, professional, civil, and criminal protection. Ultimately, the reconstruction of criminal liability for the misuse of EMRs should be oriented not only toward punishing offenders but also toward strengthening patients' rights and providing effective remedies for victims. A comprehensive legal framework should establish clear prohibited conduct, responsible subjects, standards of culpability, individual and institutional accountability, reliable digital evidence, proportionate sanctions, and effective patient remedies. Such reconstruction is essential to strengthen legal protection, ensure legal certainty, enhance accountability in digital healthcare management, and build public trust in the secure and responsible use of Electronic Medical Records.

REFERENCES

A. Books

1. Fuady, M. (2013). *Teori-teori besar (grand theory) dalam hukum*. Kencana.
2. Hamzah, A. (2017). *Hukum pidana Indonesia*. Sinar Grafika.
3. Marzuki, P. M. (2017). *Penelitian hukum* (Edisi revisi). Kencana.
4. Nasution, B. (2014). *Hukum kesehatan: Pertanggungjawaban dokter*. Rineka Cipta.
5. Prasetyo, T. (2016). *Hukum pidana*. Rajawali Pers.
6. Rahardjo, S. (2000). *Ilmu hukum*. PT Citra Aditya Bakti.
7. Ratman, H. D. (2018). *Aspek hukum informed consent dan rekam medis dalam transaksi terapeutik* (Ed. ke-2). Keni Media.
8. Rizkia, N. D., & Fardiansyah, H. (2023). *Metode penelitian hukum (normatif dan empiris)*. Widina Bhakti Persada Bandung.
9. Soekanto, S., & Mamudji, S. (2015). *Penelitian hukum normatif: Suatu tinjauan singkat*. Rajawali Pers.
10. Soerjono Soekanto. (2016). *Pengantar penelitian hukum*. UI Press.
11. Triwibowo, C. (2012). *Perizinan dan akreditasi rumah sakit: Sebuah kajian hukum kesehatan*. Nuha Medika.
12. Wignjosoebroto, S. (2013). *Hukum: Konsep dan metode*. Setara Press.
13. Widodo, E. (2019). *Hukum pidana dan pertanggungjawaban pidana*. Rajawali Pers.

B. Journals

1. Dady, R. D. (2026). *Perlindungan hukum data pribadi pasien pada rekam medis elektronik: Analisis hukum Kesehatan Indonesia. Glosains: Jurnal Sains Global Indonesia, 7*(2). https://doi.org/10.59784/glosains.v7i2.680
2. Magdalena, M., Sarwo, Y. B., & Wibowo, D. B. (2024). *Perlindungan hukum bagi pasien terhadap hak akses rekam medis elektronik di rumah sakit paska Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis. Soepra Jurnal Hukum Kesehatan*.
3. Punia, I. G. E. A. A. (2024). *Aspek hukum dan pertanggungjawaban keamanan data rekam medis elektronik di Indonesia. Jurnal Kesehatan, 1*(1).
4. Saputra, T. E. (2024*). Penggunaan rekam medis elektronik dalam mewujudkan perlindungan hukum keamanan data pribadi pasien. Fundamental: Jurnal Ilmiah Hukum, 13*(2), 57–75. https://doi.org/10.34304/jf.v13i2.276
5. Siregar, R. A., & Sinaga, H. S. R. (2025). *Aspek hukum perlindungan data pasien dalam penyelenggaraan rekam medis elektronik di Indonesia. Jurnal Hukum to-ra: Hukum untuk Mengatur dan Melindungi Masyarakat, 11*(1), 106–116. https://doi.org/10.55809/tora.v11i1.433
6. Sudjana, S. (2017). *Aspek hukum rekam medis atau rekam medis elektronik sebagai alat bukti dalam transaksi terapeutik. Veritas et Justitia, 3*(2). https://doi.org/10.25123/vej.2685
7. Shah, S. M., & Khan, R. A. (2020). Secondary use of electronic health record: Opportunities and challenges. *Journal of Health Informatics*.

C. Peraturan Perundang-undangan

1. Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 tentang *Kesehatan.*
2. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang *Pelindungan Data Pribadi.*
3. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang *Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.*
4. Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang *Rekam Medis.*
5. Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang *Penyelenggaraan Sistem dan Transaksi Elektronik.*