HORIZON PUBLIC LEGAL STUDIES
Vol 2 Issue 1 Tahun 2025
Doi : https://doi.org/10.56087/xg3ptf55

Criminal Act of Misuse of Patient Medical Data Against Health Insurance

Sukaina Aziilah[1], Muhammad Fauzi Ramadhan[2], Tri Abriana Ma'ruf[3].

[1,2,3] Fakultas Hukum, Universitas Muslim Indonesia, Indonesia

Surel Koresponden: Sukainaaziilah@gmail.com

Abstrak: Penelitian ini bertujuan untuk menganalisis tindak pidana penyalahgunaan data medis pasien dalam konteks asuransi kesehatan di Indonesia, yang merupakan isu krusial dalam perlindungan hak privasi individu. Dalam praktiknya, tidak jarang terjadi penyalahgunaan data medis, baik secara langsung maupun tidak langsung, yang dapat merugikan pasien secara fisik, psikologis, maupun secara finansial. Penelitian ini menggunakan pendekatan yuridis dengan menelaah kerangka hukum yang berlaku, serta dikombinasikan dengan studi kasus sebagai pendekatan empiris untuk menilai implementasi hukum dilakukan di lapangan. Hasil penelitian ini meskipun terdapat kerangka hukum yang mengatur tentang perlindungan data medis, dalam pelaksanaannya masih harus menghadapi berbagai tantangan, seperti lemahnya pengawasan, rendahnya literasi hukum, serta belum adanya mekanisme sanksi yang tegas dan efektif. Penelitian ini memberikan sejumlah rekomendasi strategis untuk memperkuat perlindungan hukum terhadap data medis pasien, antara lain melalui harmonisasi regulasi, peningkatan pengawasan, edukasi bagi pemangku kepentingan, serta pembentukan lembaga pengawas independen yang berwenang dalam perlindungan data pribadi di sektor kesehatan dan asuransi.

Kata Kunci: Penegakan Hukum, Penyalahgunaan Data Medis, Penipuan Asuransi, Rumah Sakit, Perlindungan Data Pribadi.

Abstract: *This study This study aims to analyze the criminal misuse of patient medical data in the context of health insurance in Indonesia, which is a crucial issue in protecting individual privacy rights. In practice, misuse of medical data is not uncommon, both directly and indirectly, which can harm patients physically, psychologically, and financially. This study uses a normative juridical approach by examining the applicable legal framework, combined with case studies as an empirical approach to assess how the law is implemented in the field. The results show that although a legal framework governing medical data protection exists, its implementation still faces various challenges, such as weak oversight, low legal literacy among data holders, and the absence of a firm and effective sanction mechanism. This study provides several strategic recommendations to strengthen legal protection for patient medical data, including through regulatory harmonization, increased oversight, education for stakeholders, and the establishment of an independent supervisory body authorized to protect personal data in the health and insurance sectors.*

Keywords: *law Enforcement, Misuse of Medical Data, Insurance Fraud, Hospital, Personal Data Protection.*

A. INTRODUCTION

The digital era has brought about a major transformation in the healthcare system, particularly in the management of patient medical data. In this digital era, technological applications increasingly dominate almost all aspects of human life, including the healthcare sector. One particularly sophisticated technology in the healthcare sector is the E-Medical Record application. In the context of modern healthcare, medical data not only serves as documentation of a patient's medical history but also plays a crucial role in various administrative matters, including health insurance claims.[1] Medical data protection is crucial to ensure patient safety and well-being. Hospitals are required to ensure that their medical data systems are secure and protected from various potential threats. However, the potential for misuse of medical data for improper purposes is increasing, particularly in cases of insurance claim fraud.[2]

In Makassar, a metropolitan city located in the South Sulawesi province of Indonesia with a rapidly growing healthcare sector, cases of misuse of patient medical data are showing a worrying trend.[3] According to data from the Makassar Police, throughout 2023, there were 17 cases of insurance fraud involving the misuse of patient medical data, with total losses reaching IDR 2.3 billion. This figure represents a 40% increase compared to the previous year. Police investigations have revealed increasingly sophisticated modus operandi, involving organized networks comprising hospital employees, insurance agents, and even document forgery syndicates.[4]

The reality on the ground (das sein) indicates that the implementation of medical data security systems in various hospitals in Makassar City remains suboptimal. A 2023 audit by the Makassar City Health Office revealed that of the 12 hospitals surveyed, only four had data security systems that met standards. This is a serious concern, as poorly protected patient medical data can compromise patient privacy and security. More intensive training for hospital staff on the importance of maintaining data security, increased internal oversight, and the implementation of strict sanctions for violators can help reduce the risk of future medical data misuse.[5]

This situation is in stark contrast to the ideal state of affairs (das sollen), where patient medical data must be managed securely and responsibly in accordance with Ministerial Regulation No.

269 of 2008 concerning Medical Records and Law No. 29 of 2004 concerning Medical Practice. The regulation clearly stipulates the obligation to maintain the confidentiality of patient medical data and the sanctions for violators. Furthermore, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions also provides a legal basis for prosecuting cybercrimes related to personal data.[6]

Medical confidentiality is both a right and an obligation inherent to every patient. Medical confidentiality not only reflects respect for individual privacy but is also an integral part of ethical and legal doctrine in medical practice, serving as a crucial link in the implementation of medical procedures within healthcare services.[7] Therefore, maintaining the confidentiality of medical data is a key foundation for building a trusting relationship between patients and healthcare institutions. Therefore, proper management of patient medical data in accordance with the principle of legal prudence is expected to further ensure the security of personal health information and provide maximum benefits for all parties involved.[8]

The research questions discussed in this study relate to the legal aspects of the criminal act of misusing health insurance patients' medical data and the legal consequences of misusing health insurance, which will be addressed in the results and discussion sections.

B. METOD

The method used in this research is the normative legal method, namely by conducting a literature study that includes the use of primary, secondary, and tertiary legal materials. In this normative legal research, the author examines legal principles that depart from legal systematics by first identifying legal rules that have been formulated in legislation. Legal materials are collected through reading and analyzing various related literature, discussions, and reviewing books, laws and regulations, documents, and other research results, both in print and electronic form, including searches via the internet.[9] Secondary legal materials are explanations of primary legal materials, while tertiary legal materials are used to help explain and facilitate understanding of primary and secondary legal materials, such as legal dictionaries, the Great Indonesian Dictionary, and English dictionaries.

C. DISCUSSION

Based on data obtained by the author from normative legal materials, including the following:

1. Legal Aspects of Criminal Acts of Misuse of Patient Medical Data Against Health Insurance

In the Criminal Code (KUHP), criminal acts are known as Strafbaarfeit. The term Strafbaarfeit refers to a punishable event or act. A criminal act is a basic concept in criminal law (normative juridical) relating to acts that violate criminal law. A criminal act is a legal term referring to acts or omissions prohibited by law and punishable by criminal sanctions. Criminal acts also include insurance fraud, which is a serious violation under criminal law.[10]

In the context of crimes involving technology and data, such as cases of misuse of medical data in insurance fraud, law enforcement faces more complex challenges. This is because crimes often involve digital technology, personal data management, and regulations that evolve with the times. The criminal act of misuse of medical data for health insurance can be subject to criminal sanctions under the provisions of the Criminal Code (KUHP) and more specific laws, such as the Electronic Information and Transactions Law and the Health Law. Misuse of medical data can be categorized as fraud or a violation of a person's personal rights.[11]

The crime of falsifying medical data or disclosing a patient's medical information without authorization for unlawful purposes. The legal aspects governing the misuse of medical data can be viewed from several perspectives, including criminal law, health law, and personal data protection.[12] The use of medical data for healthcare services illustrates contemporary bioethical principles that prioritize health information management. The individual's right to privacy remains a fundamental principle. Access to medical information should only be granted to those directly involved in patient care.[13]

In today's digital era, technology is advancing rapidly, becoming an essential part of human life. With these technological developments, new methods of healthcare services have emerged, namely telemedicine, which utilizes technological media to reduce face-to-face

contact between doctors and patients. Telemedicine is a tool that can meet basic health needs. Misuse of medical records can occur if medical personnel or healthcare professionals leak, use, or access patient data without proper authorization, whether for personal gain, material gain, or other purposes unrelated to the provision of medical services. This contradicts Article 28G of the 2045 Constitution concerning the right to personal data protection, which is further regulated in Law No. 36 of 2009 concerning Health.[14]

The government aims to provide good health services to the public, thereby creating superior human resources. Health is a fundamental right for every human being. Legal protection for patients in online health services is crucial. This is understood from the provisions of Article 3 paragraphs (2) and (4) and Article 7 of Medical Council Regulation No. 47 of 2020, which apply the principle of patient confidentiality, require registration certificates and practice permits, and provide medical records. The prohibition on doctors engaging in telemedicine also serves as a form of legal protection for patients. Protection of personal data in the context of online health services is a fundamental human right. Patient data is categorized as personal data that identifies users, such as name, demographic data, telephone number, IP address, online username, sexual orientation, health data, and so on. Legal protection is an effort undertaken by law enforcement to protect human rights that have been violated by others. Forms of legal protection for the confidentiality of patient medical record data can be carried out by implementing laws and regulations relating to the protection of personal data.[15]

Law Number 11 of 2008 concerning Electronic Information and Transactions regulates the protection of personal information. Misuse of patient medical data, if done intentionally or without the patient's permission, can be categorized as a violation of privacy. In this case, if any patient medical data submitted to health insurance is used for unauthorized purposes or disseminated without permission, it can be considered a violation of the provisions of the ITE Law.[16] This law prohibits the theft of personal data and the misuse of medical data. Article 57 of Law Number 36 of 2009 concerning Health discusses maintaining the confidentiality of patient medical data. Misuse of patient medical data by health insurance companies could violate the provisions that require all parties handling patient medical data to maintain its confidentiality. If health insurance companies disclose or use patient medical

data without permission or for unauthorized purposes, this clearly violates the confidentiality principle stipulated in this Health Law.[17] Article 26 of Law Number 19 of 2016 concerning Personal Data Protection requires parties collecting, storing, and processing personal data (including medical data) to obtain permission from the data owner. This law emphasizes the importance of obtaining consent from data owners before collecting and processing personal data. If a health insurance company accesses a patient's medical data without permission, it could be considered a violation of the Personal Data Protection Law. This is increasingly relevant given the widespread digitalization of medical data involving multiple parties.

In the context of health insurance, violations of the obligation to protect participants' personal data, such as medical data, can lead to legal action. Misuse of medical data by an insurance company can be subject to administrative and criminal sanctions. The legal procedures applicable to the misuse of patient medical data by health insurance companies can involve several legal stages that refer to existing laws and regulations. Misuse of medical data constitutes a violation of patients' legally protected privacy rights, and therefore, these legal procedures will involve various steps at both the administrative and criminal levels.

There are several legal stages that must be carried out, including:

1. Reporting of Data Abuse Crimes: The reporting party is the patient or any aggrieved party, such as the patient's family or a related organization. The basis for the report may be an alleged violation of personal data protection laws, a breach of medical confidentiality, or data misuse.
2. Investigation and Probe, in this case, the police will collect evidence to determine whether there has been misuse of medical data and who is responsible, further investigation if the evidence found indicates misuse of medical data, then the investigation process will be continued to find out the perpetrator and the modus operandi of the misuse.
3. Prosecution and Court Examination: If sufficient evidence is found that the misuse of medical data violates criminal law, the public prosecutor can submit the case to court for examination and trial. Depending on the type of violation identified, criminal penalties may include fines or imprisonment. For example, in cases of misuse of

personal data that harms another party, the perpetrator may be subject to criminal penalties under the ITE Law or the Personal Data Protection Law.

4. Compensation or Civil Claims: In addition to criminal or administrative sanctions, victims of medical data misuse can also file a claim for compensation for losses incurred as a result of the misuse, either against the insurance company or a third party involved. These civil claims will be processed in district court by filing a lawsuit to obtain financial compensation for the losses suffered.

Thus, the legal process for misuse of patient medical data by health insurance companies involves several stages, including criminal investigations, administrative sanctions, and potential civil lawsuits and compensation. All of this aims to protect patients and ensure accountability in the management of medical data by insurance companies.

2. Legal Consequences of Health Insurance Abuse.

The legal consequences of health insurance misuse include various consequences depending on the type of violation and the parties involved. Misuse of health insurance, whether by patients, healthcare providers, or insurance companies, can result in various legal consequences, including criminal, civil, and administrative ones.[18]

From a criminal legal perspective, misuse of insurance claims, such as submitting false claims, manipulating medical data, or transferring inappropriate treatment costs, can be subject to fraud. In Indonesia, fraud is regulated by the Criminal Code (KUHP), and perpetrators are subject to imprisonment and/or fines. For example, Article 378 of the Criminal Code states, "Anyone who, with the intent to unlawfully benefit themselves or another person, by using a false name or false status, by deception, or by a series of lies, induces another person to hand over any property to them, or to grant a loan or to cancel a debt, shall be guilty of fraud and be punished by a maximum imprisonment of four years." Meanwhile, in cases of personal data misuse, health insurance misuse involving the leaking or use of patient medical data without permission or for unauthorized purposes, the perpetrator can be prosecuted under Law Number 27 of 2022 concerning Personal Data Protection. The sanctions under this regulation include a maximum imprisonment of 5 (five) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).

The civil law perspective on health insurance misuse can also lead to civil legal consequences, particularly those related to losses arising from the misuse. Some potential civil legal consequences include compensation. If a health insurance company rejects a legitimate claim without proper justification or misuses a patient's medical data, the injured party can sue in court for compensation for the losses or intangible damages suffered. If health insurance misuse involves a breach of contract or insurance, the insurance company or other involved parties may be subject to civil liability. Patients can seek fulfillment of contractual obligations or compensation for the breach.[19]

Medical personnel or healthcare providers involved in health insurance misuse may be subject to administrative sanctions by the Ministry of Health or their professional organizations, such as the Indonesian Medical Association. These sanctions include revocation of their practice licenses or demotion of their professional status. Misuse of medical data involving the abuse of health facilities or insurance providers can result in administrative sanctions from BPJS Kesehatan or termination of cooperation with the health facility. Misuse of health insurance can damage the reputation and public trust in health insurance providers and healthcare providers.

D. CONCLUSION

The legal aspects of the criminal act of misuse of patient medical data by health insurance companies include violations of several statutory provisions. This misuse is classified as a criminal act because it is related to fraud, data theft, violation of privacy, and violation of medical ethics. Efforts to prevent and enforce the law against medical data misuse must be carried out in an integrated manner between the government, hospitals, insurance companies, law enforcement officials, and the public. Education, improving data security systems, and enforcing legal sanctions are concrete steps that must be optimized. From the conclusions, some recommendations can be provided that are expected to improve regulations related to the management and protection of patient medical data, especially in aspects related to digital technology and electronic data.

E. REFERENCE

[1] Dwi Dasa Suryantoro, "TINJUAN YURIDIS TERHADAP PERATURAN MAHKAMAH AGUNG NOMOR 1 TAHUN 2016 TENTANG MEDIASI," *Leg. Stud. J.*, vol. 3, no. 2, pp. 91–110, Feb. 2023.

[2] O. Y. Disalahgunakan and H. Y. Rumengan, "No Title," vol. 14, 2024.

[3] I. A. Chandra *et al.*, "Jurnal Pendidikan dan Pengajaran PERLINDUNGAN DATA PRIBADI DALAM MENCEGAH TINDAK PIDANA PENYALAHGUNAAN HAK PASIEN Jurnal Pendidikan dan Pengajaran," vol. 6, no. 2, pp. 32–45, 2025.

[4] D. P. Setiawan, "Penyalahgunaan Data Pribadi Pasien Dalam Rekam Medis Oleh Tenaga Medis / Tenaga Kesehatan Rumah Sakit," vol. 2, no. 4, pp. 674–680, 2024.

[5] Meray Hendrik Mezak, "Jenis, Metode dan Pendekatan Dalam Penelitian Hukum," *Law Rev.*, vol. 5, no. 1, pp. 85–97, Mar. 2006.

[6] Fitra Dewi Nasution Ferry Aries Suranta, "PENYELESAIAN SENGKETA PERDATA DENGAN MEDIASI MENURUT PERATURANMAHKAMAH AGUNG NOMOR 1 TAHUN 2008," *Mercatoria*, vol. 5, no. 1, pp. 35–46, Jan. 2012.

[7] F. H. A. D. W. L. Rendi Gue, "KEKUATAN HUKUM AKTA PERDAMAIAN DALAMKASUS PERCERAIAN MELALUI MEDIASI DIPENGADILAN MENURUT PERSPEKTIF HUKUMPERDATA," *Lex Priv.*, vol. 11, no. 2, Feb. 2023.

[8] N. A. Sinaga and T. Zaluchu, "PERLINDUNGAN HUKUM HAK-HAK PEKERJA DALAM HUBUNGAN KETENAGAKERJAAN DI INDONESIA," Indonesia, Jan. 2017. doi: https://doi.org/10.35968/jti.v13i1.

[9] M. Syarif, D. S. Busthami, M. K. Hidjaz, and A. Aswari, "Metode Penelitian Hukum (Legal Research Methods)," no. 1, 2017.

[10] D. G. Yambo, L. Marsuni, and A. Aswari, "Legal Force of Information Technology-Based Money Lending Agreements," vol. 1, no. 2, pp. 1–8, 2025.

[11] M. F. Ramadhan, A. Asis, and A. M. Muin, "Law Enforcement Of The Crime Of Illegal Fishing In The Waters Area Of Pangkajene Regency And The Islands," *Leg. Br.*, vol. 11, no. 3, pp. 2722–4643, 2022, doi: 10.35335/legal.

[12] R. Ramadani, "PROTEST VOTE : MITIGATING THE IMPACT OF SINGLE CANDIDATES," vol. 10, no. 1, pp. 85–104, 2025, doi: 10.14710/dilrev.10.1.2025.85-

104.

[13] S. Indiva, K. Ahmad, and H. Djanggih, "Peran Dan Fungsi Jaksa Sebagai Penyidik Dalam Proses Pemeriksaan Tindak Pidana Korupsi," vol. I, no. I, pp. 1–16, 2025.

[14] I. Abbas, R. Ramadani, and U. M. Indonesia, "Yustisia Jurnal Hukum Balancing State Revenue and Fair Competition in Social Commerce Platforms," vol. 14, no. 2, pp. 170–185, 2025, doi: 10.20961/yustisia.v14i2.93969.

[15] A. Aswari, "Peran Ganda Administrator sebagai Mediator dalam Sengketa Transaksi Ponsel Bekas secara Online," *J. Ilm. Kebijak. Huk.*, vol. 12, no. 3, p. 259, Dec. 2018, doi: 10.30641/kebijakan.2018.v12.259-274.

[16] S. Bachri and N. Azisa, "Optimizing the Management of Seized Goods : The Strategic Role of the Prosecutor ' s Office in Asset Recovery from Corruption Crimes," vol. 3, no. 2, pp. 3184–3203, 2025.

[17] M. A. Munandar *et al.*, "Menilik Sanksi Pidana Tambahan Pemenuhan Kewajiban Adat Setempat dalam KUHP Nasional," vol. 27, 2025, doi: 10.30595/pssh.v27i.1842.

[18] A. Firman, "How Digital Technology Driven Millennial Consumer Behaviour in Indonesia."

[19] Y. Sukma Permana, "PERJANJIAN JUAL-BELI MELALUI E-COMMERCE DI DITINJAU DARI HUKUM PERJANJIAN DI INDONESIA".