

LEGAL ASPECTS OF DISCLOSING PATIENT DATA UNDER ELECTRONIC INFORMATION AND TRANSACTION LAW

Mustika Chasanatusy Syarifah^{1,2,3,*}, Diana Arum Lisnawati²

¹*Universitas Hang Tuah Surabaya, Faculty of Law, Master of Law in Health Concentration, Indonesia*

²*Universitas Nahdlatul Ulama Surabaya, Department of Forensic and Medicolegal, Faculty of Medicine, Indonesia*

³*Forensic Pathologist, RS Bhayangkara H.S. Samsoeri Mertojoso, Surabaya, Indonesia*

Abstract: In the contemporary digital landscape, the imperative for transparency in information dissemination serves to uphold the public's right of access. One dilemma that arises is the Disclosure of patients' data with the COVID-19 outbreak, which can help to prevent transmission but also risks violating patient privacy. For example, the patient's address, although not medical data, is closely related to medical records and can be considered medical data in a pandemic. This combination of personal and medical data needs to be further explained in Indonesian law, especially the Electronic Information and Transactions Law (EIT Law). This study aims to analyze the legal aspects of disclosing patient personal data for public interest in an infectious outbreak based on the EIT Law. The method used is normative juridical. Secondary data is collected from relevant legal sources. In a public health emergency, specific personal data may be disclosed for the public interest per the Health Law and the Law on Public Information Disclosure provisions. The Disclosure shows that to combat the outbreak, personal data can be treated as medical data necessary to support public safety. As a solution, authorities can use an anonymous disclosure mechanism to balance the public interest and the patient's data rights. Disclosure of patient personal data, such as patient addresses for tracing purposes during the pandemic, does not violate the EIT Law because it is permitted for the public interest and national resilience. With the enactment of the Personal Data Protection Law, personal data protection becomes more comprehensive.

Keywords: patient confidentiality, electronic medical record, law of electronic information and technology, law of personal data protection.

INTRODUCTION

The ever-growing advancement of digital technologies in healthcare has offered innovative solutions to various challenges in healthcare systems. These developments have also increased the quantity and diversity of digital interactions and personal health information generated and collected within and outside traditional healthcare environments (1). Along with technological development, the medical record recording system has transformed from a conventional physical to an electronic format (2). This change raises various issues, including data security aspects, infrastructure readiness, and adequate regulations to

support the implementation of Electronic Medical Records (EMR) (3). In response to these challenges, the government issued the Minister of Health Regulation Number 24 of 2022 provide legal certainty in implementing electronic medical record systems in healthcare facilities (4). Managing EMR is a crucial issue in health sector, especially regarding patient data confidentiality (5).

In today's digital information era, transparency in reporting an event is necessary for the public to know to ensure access to information. However, the demand for openness can indirectly blur the boundaries between individual privacy and public interest (6). A central legal dilemma in the context of pandemic

*Correspondence to: Mustika Chasanatusy Syarifah, dr., Sp.FM.,MH., Jalan Raya Jemursari No. 51 – 57, Surabaya, Indonesia, E-mail: mustika4n6@unusa.ac.id

concerns the disclosure of patients' personal data to the public. While such disclosure may enhance the effectiveness of contact tracing and mitigate the risk of viral transmission, it simultaneously raises significant concerns regarding the protection of individual privacy rights, which are safeguarded by the state as part of broader data protection obligations (7).

In an infectious disease outbreak such as COVID-19, patient addresses must be disclosed to the public for tracing purposes. Although the patient's residence is not included in the category of medical data, the patient's address is closely related to the medical record. In a situation of an infectious pandemic disease, the patient's address, which was originally personal data, can eventually be considered as medical data. This intersection between personal and medical data must be clarified in Indonesian law and linked to the Electronic Information and Transactions Law (EIT Law). The purpose of this article is to analyze the legal aspects related to the disclosure of patient personal data for the public interest, especially in the context of infectious disease tracing, and to evaluate the extent to which personal data protection is by the provisions stipulated in the EIT Law.

METHOD

This study employs a normative legal research methodology (doctrinal research), wherein secondary data is gathered from pertinent legal sources and normative frameworks, including statutes, regulations, legal theories, judicial decisions, and the doctrinal perspectives of prominent legal scholars (8).

DISCUSSION

1. Legal Aspects of Privacy and Confidentiality in Electronic Medical Records

a) Privacy and Confidentiality

Privacy and confidentiality are related, but they are two different things. Confidentiality regulates who is authorized to access information, while privacy relates to an individual's right to control when, how, and to what extent personal information can be shared or accessed (9). Confidentiality protects patient information from unauthorized parties during storage and transmission. The protection can be achieved through encryption and password-protected system access to keep data safe from unauthorized changes or deletions (10).

Ownership of medical records is regulated in Medical Practice Law Number 29 of 2004 Article 47

Paragraph 1, physical medical record files become the property of Health Service Facilities (11). Meanwhile, pursuant to Article 26, Paragraph 1 of Minister of Health Regulation Number 24 of 2008, the contents of medical records are considered the property of the patient, thereby granting the patient the right to access and request a copy of their medical information (12). With the ownership status of the contents of medical records, the patient can be considered to have entrusted his/her personal and health information stored in the medical record files to Health Service Facilities and health workers authorized to access them (13).

Medical records contain two main types of information: medical and non-medical. According to Guwandi in the book "Trilogi Rahasia Medis", complete medical records include four data types. First, personal data such as name, identity number, place/date of birth, gender, marital status, address, and other identification information. Second, financial data such as insurance policy number. Third, social data, including citizenship/nationality. Finally, medical data, including physical examination results, medical history, treatment, treatment progress, health worker instructions, and other reports related to patient care and treatment (14). In addition to containing medical and non-medical information, EMR are also related to informed consent. Informed means receiving an explanation or information, while consent means giving approval or permission. Thus, informed consent can be interpreted as consent given voluntarily and rationally by the patient after receiving and understanding the information conveyed by the doctor (15).

In international practice, such as at the National University Health System and Yishun Community Hospital in Singapore, patients who voluntarily provide personal data to obtain medical care are deemed to have consented to the collection, use, disclosure, and processing of such data for medical service purposes (16, 17).

b) Legal Aspects of Patient Privacy and Confidentiality in Electronic Medical Records

According to the Indonesian Medical Council's Medical Record Guidelines, doctors and dentists must maintain the confidentiality of patients' medical history. Disclosure of medical secrets is only permitted for the benefit of the patient, at the request of law enforcement officers, the patient themselves, or by statutory provisions (18).

Health Law Number 17 of 2023 Article 296 Paragraph 5 and Article 297 Paragraph 3 state that medical records must be stored and maintained by

medical personnel, health workers, and heads of health facilities. Health service providers are legally obligated to safeguard the confidentiality, security, integrity, and availability of information contained within medical records, in accordance with applicable regulatory standards (19).

Pursuant to Article 32 of the Minister of Health Regulation No. 24 of 2022, all parties engaged in the provision of healthcare services within Health Service Facilities are mandated to uphold the confidentiality of medical record contents, irrespective of the patient's survival status, including after the patient's death (20). In addition, Article 4 of the Minister of Health Regulation Number 36 of 2012 requires that everyone engaged in delivering medical services and/or managing patient data and information must maintain the confidentiality of medical information (21).

2. Exceptions to Confidentiality: Disclosure of Patient Personal Data

The protection of patient data confidentiality constitutes both a legal requirement and an ethical responsibility for hospitals, which function as healthcare providers and custodians of electronic medical records. Nonetheless, under specific conditions, the disclosure of medical information may be deemed legally permissible when justified by the public interest, particularly in the context of public health emergencies, such as those occurring during a pandemic (22).

According to Public Information Disclosure Law Number 14 of 2008 Article 6 Paragraph 3, one of the points of public information that cannot be provided or opened by a Public Agency is information related to personal rights (23). However, in a specific domain, a critical legal challenge emerges concerning information disclosure, wherein two fundamental interests converge: the protection of individual privacy rights and the obligation to uphold the public's right to access information that bears significance for the broader public interest. Legal issues related to the provision of medical record information or patient health data are in the spotlight, especially in cases involving the disclosure of information regarding the health conditions of patients with infectious diseases, which often triggers debate between individual interests and the urgency of public health (6).

a) Disclosure of Personal Data in the Electronic Information and Transactions Law

In the EIT Law, the prohibition on disclosing personal information to the public is regulated in Article 26 Paragraph 1. This article explains that any

utilization of information through electronic media regarding an individual's data must be done with the individual's permission unless otherwise mandated by laws and regulations (24). Furthermore, individuals who feel that their privacy has been violated have the right to file a lawsuit by Article 26 Paragraph 2. This provision emphasizes that personal data may not be used or disseminated via electronic media without the consent of the individual concerned unless otherwise stipulated by laws and regulations. The regulation provides legal protection for individual privacy in the digital realm.

b) Disclosure of Personal Data in the Personal Data Protection Law

Before the Personal Data Protection Law (PDP Law), personal data protection was spread across several laws and regulations (25), one of which was in the EIT Law (26). In 2016, the Draft on Personal Data Protection was initiated. Subsequently, the PDP Law was passed on September 20, 2024, and came into effect on October 17, 2024 (27).

Article 4 of the PDP Law contains two types of personal data. First, general data contained name, gender, nationality, and religion. Then the second is specific personal data such as health information, biometrics, criminal records, and finances (28). Based on these regulations, it can be concluded that the address is included in general personal data.

Furthermore, Article 15 Paragraph 1 of the PDP Law states that the rights of Personal Data Subjects can be excluded for the interests of national defense and security (28). The Brazilian General Data Protection Law (LGPD) and the European Union General Data Protection Regulation (GDPR) stipulate that in situations involving emergencies or matters of public interest - such as public health crises - the utilization of personal data may be permitted without the necessity of obtaining prior consent from citizens. However, this is only permitted on the condition that data protection is guaranteed, the data is used appropriately for explicit and legitimate purposes, and the authorized institution to process the data meets the requirements set by applicable regulations (29).

c) National Defense and Security Interests in the Context of Infectious Disease Outbreaks

Outbreaks of infectious diseases, such as COVID-19, are a real threat to national safety and are included in the potential disasters described in Disaster Management Law Number 24 of 2007 (30). The pandemic has prompted the government to implement policies aimed at reducing physical contact

and implementing Large-Scale Social Restrictions in several regions, which have an impact on hampering productivity in various sectors. In addition to posing a threat to public health and the economy, the pandemic has also affected food sufficiency (31). The spread of the COVID-19 virus is considered a threat to national interests, so handling it is part of efforts to maintain national resilience (32).

3. Legal Aspects of Disclosure of Personal Data for Public Interest

Article 4, Paragraph 4 of Health Law Number 17 of 2023 stipulates that the right to the confidentiality of personal health data and information may be waived under specific circumstances, including in cases of extraordinary events, epidemics, disasters, or when necessary to safeguard public safety from imminent threats (19). Article 10 of Public Information Disclosure Law Number 14 of 2008 stipulates that public bodies must immediately announce information that could threaten many people's lives and public order (23).

Information regarding COVID-19 patient data, such as residential addresses and treatment locations, must be transparently disclosed to parties handling the outbreak. Specific personal data can be treated as medical data in a public health emergency to support efforts to control the outbreak (33). The disclosure of medical information for COVID-19 patients aims to enable the public to discover the domicile and social interaction history of patients or suspected COVID-19 (22). In response to the risk of personal data misuse during the COVID-19 public health emergency, the Central Information Commission of Indonesia issued Circular Letter Number 2 of 2020 concerning Public Information Services. This regulation delineates the boundaries of publicly accessible information, specifically limiting it to essential details such as the type of disease, transmission patterns, epicenter locations, and prevention measures. The disclosure of such data is subject to strict procedural safeguards to ensure the protection of individual privacy, particularly for Persons Under Monitoring, Patients Under Surveillance, confirmed COVID-19 cases, and recovered individuals (34).

Anonymized data, having been stripped of identifiers to the extent that individuals can no longer be identified, is generally excluded from the definition of personal data under data protection frameworks. Conversely, pseudonymized data remains classified as personal data, as the presence of reversible key codes retains the potential for re-identification, thereby posing

a significant security risk (35). Under data protection law, anonymized or aggregated data is generally not classified as personal data, as it no longer permits the identification of specific individuals. Nevertheless, the collection of such data - particularly regarding geographic location, ethnicity, health status, or socio-economic conditions - may still result in adverse implications for identifiable groups. Accordingly, ethical scrutiny is essential to assess whether the potential benefits derived from the use of such data justify the associated risks (36).

The use of patient ownership rights over the contents of medical records by the government does not require patient consent as long as other patient rights, such as the right to privacy, are respected (13). In the context of the COVID-19 pandemic, this is important because COVID-19 patient data is needed to monitor the development and spread of the virus nationally (37).

In conclusion, disclosure of patient personal data, especially patient addresses, for tracing purposes in the context of the COVID-19 pandemic, cannot be considered a violation of the EIT Law. Disclosing personal data for the public interest, such as preventing the spread of infectious diseases, is justified within the framework of public interest and national resilience. In addition, with the enactment of the PDP Law, the provisions in the EIT Law regarding personal data protection become less relevant because the PDP Law provides more specific and comprehensive protection for personal data. As a solution, the authorities can implement a mechanism for anonymously disclosing patient personal data to maintain a balance between the public interest and protecting patients' personal data rights.

Conflict of interest

The authors declare that they have no conflict of interest.

References

1. Rockwern B, Johnson D, Snyder Sulmasy L. Health Information Privacy, Protection, and Use in the Expanding Digital Health Ecosystem: A Position Paper of the American College of Physicians. *Ann Intern Med.* 2021; 174(7): 994-998.
2. Sholkan M. Implementasi Rekam Medis Elektronik Dan Kajian Hukumnya. *Konstitusi: Jurnal Hukum, Administrasi Publik, dan Ilmu Komunikasi.* 2024; 1(3): 39-54.
3. Indra T, Dewi N, Wibowo D. Perlindungan Kerahasiaan Data Pasien vs Kewajiban Membuka Akses Rekam Medis Elektronik. *SOEPRA Jurnal Hukum Kesehatan.* 2024; 10(1): 97-117.
4. Siregar R.A. Penerapan Permenkes Nomor 24 Tahun 2022

- Tentang Rekam Medis Terhadap Efektivitas Pelayanan Kesehatan. *Jurnal Ilmu Hukum Kyadiren*. 2024; 5(2).
5. Ardiansyah MR, Ardiana R. Kewajiban Dan Tanggung Jawab Hukum Perdata Dalam Perlindungan Privasi Data Pasien Dalam Layanan Kesehatan Digital. *Hakim: Jurnal Ilmu Hukum dan Sosial*. 2023; 1(4): 276-287.
 6. Prananda RR. Batasan Hukum Keterbukaan Data Medis Pasien Pengidap Covid-19: Perlindungan Privasi VS Transparansi Informasi Publik. *Law, Development & Justice Review*. 2020; 3(1): 142-168.
 7. Sihombing ENAM, Hadita C, Syaputra MYA. Legal Securities Against Covid-19 Patient Privacy Data in Indonesia. *Veteran Law Review*. 2021; 4(1): 34-49.
 8. Tan D. Metode Penelitian Hukum: Mengupas dan Mengulas Metodologi dalam Menyelenggarakan Penelitian Hukum. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*. 2021; 8: 2463-2478.
 9. Tertulino R, Antunes N, Morais H. Privacy in electronic health records: a systematic mapping study. *J Public Health (Bangkok)*. 2024; 32(3): 435-454.
 10. Hassan M, Butt MA, Zaman M. Privacy Preserving Data Mining for Healthcare Record: A Survey of Algorithms. *International Journal of Trend in Scientific Research and Development*. 2017; 2(1): 1176-1184.
 11. Pemerintah Pusat, Lembaran Negara Republik Indonesia tahun 2004 Nomor 116 Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran. Indonesia, 2004.
 12. Kementerian Kesehatan, Permenkes Nomor 24 Tahun 2008 tentang Rekam Medis Pasal 26 Ayat 1. Indonesia, 2008.
 13. Kurniawan AL, Setiawan A. Perlindungan Data rekam Medis Sebagai Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi COVID-19,” *Jurnal Hukum dan Pembangunan Ekonomi*. 2021; 9(1): 95-112.
 14. Ramadianto AY. Hak Milik Pasien Atas Isi Rekam Medis (Suatu Pendekatan Filosofis dan Hukum Perdata). *Simbur Cahaya*. 2020: 131-158.
 15. Mannelli C. Two Senses of Informed Consent. 2021: 19-30.
 16. Yishun Community Hospital. Personal Data Protection Act Notice. Accessed: Apr. 30, 2025. (Online). Available: <https://www.yishuncommunityhospital.com.sg/pages/pdpa-declaration.aspx>
 17. National University Health System, “Personal Data Protection Act.” Accessed: Apr. 30, 2025. (Online). Available: <https://www.nuhs.edu.sg/personal-data-protection-act>
 18. Hanafiah JM, Amir A, Sukatendel K. *Etika Kedokteran & Hukum Kesehatan*, 6th ed. Penerbit EGC, 2023.
 19. Pemerintah Pusat, Lembar Negara Republik Indonesia Nomor 6887 Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan. Indonesia, 2023.
 20. Kementerian Kesehatan, Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik Pasal 32. Indonesia, 2022.
 21. Kementerian Kesehatan, Peraturan Menteri Kesehatan Nomor 36 Tahun 2012 tentang Rahasia Kedokteran. Indonesia, 2012.
 22. Eria Blencisca T, Nuriyatman E. Pembukaan Rahasia Medis Pasien Covid-19 Sebagai Implementasi Di Era New Normal Dalam Pelayanan Kesehatan. *Mendapo: Journal of Administrative Law*, vol. 2, no. 2, pp. 86–98, Jun. 2021, doi: 10.22437/mendapo.v2i2.11402.
 23. Pemerintah Pusat, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61 Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik. Indonesia, 2008.
 24. Pemerintah Pusat, Lembaran Negara Republik Indonesia Nomor 4843 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Indonesia, 2008.
 25. Jannah LM. UU Perlindungan Data Pribadi dan Tantangan Implementasinya. Accessed: Apr. 28, 2025. (Online). Available: <https://fia.ui.ac.id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/>
 26. Mochtar MB. Kepastian Hukum Atas Kebocoran Data Pribadi Pengguna Aplikasi Online. *Yustisia merdeka: Jurnal Ilmiah Hukum*. 2023; 9 (2).
 27. Pratomo Y. UU Perlindungan Data Pribadi Berlaku Sepenuhnya di Indonesia. Accessed: Apr. 28, 2025. (Online). Available: <https://tekno.kompas.com/read/2024/10/18/13483697/uu-perlindungan-data-pribadi-berlaku-sepenuhnya-di-indonesia/>
 28. Pemerintah Pusat, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196 Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Indonesia, 2022.
 29. European Union, “General Data Protection Regulation.” Accessed: Apr. 25, 2025. (Online). Available: <https://gdpr-info.eu/>
 30. Pemerintah Pusat, “Lembaran Negara Republik Indonesia Tahun 2007 Nomor 66 Undang-undang Nomor 24 Tahun 2007 tentang Penanggulangan Bencana,” Indonesia, 2007.
 31. Wismayana WM, Pinatih NKDA. Pandemi dan Tantangan Ketahanan Nasional Indonesia: Sebuah Tinjauan Kritis. *Jurnal Lemhannas RI*. 2022; 8(2): 93-100.
 32. Samudro EG, Madjid MA. Pemerintah Indonesia Menghadapi Bencana Nasional Covid-19 Yang Mengancam Ketahanan Nasional. *Jurnal Ketahanan Nasional*. 2020; 26(2): 132.
 33. Lintang K, Triana Y. Perlindungan Hukum Terhadap Hak Privasi dan Rekam Medis Pasien Pada Masa Pandemi COVID-19. *Jurnal Hukum Lex Generalis*. 2021; 2(10): 913-927.
 34. Komisi Informasi Pusat, Surat Edaran Komisi Informasi Pusat Republik Indonesia Nomor 2 Tahun 2020 Tentang Pelayanan Informasi Publik Dalam Msa Darurat Kesehatan Masyarakat Akibat Corona Virus Disease 2019 (COVID-19). Indonesia, 2020.
 35. Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun*. 2019;10(1):3069.
 36. Almeida BA, Doneda D, Ichihara MY, Barral-Netto M, Matta GC, Rabello ET, Gouveia FC, Barreto M. Personal data usage and privacy considerations in the COVID-19 global pandemic. *Cien Saude Colet*. 2020;25(suppl 1):2487-2492. Portuguese, English.
 37. Hakam F. Analisis Penyediaan Rekam Medis Pasien Rawat Jalan Berdasarkan Standar Operasional Prosedur (SOP) Di Puskesmas X. *Jurnal Manajemen Informasi dan Administrasi Kesehatan (JMIK)*. 2018; 1(1).