Legal Protection of the Confidentiality of Patient Health Data in Physiotherapy Services

Dwi Selviany, Sutiarnoto, Muhammad Arif Sahlepi

Abstract

The electronic medical record (EMR) makes the data of physiotherapy patients easy to store and share, but also easy to leak. This study analyses how the confidentiality of patient health data is protected in physiotherapy services and what legal duties physiotherapists have to keep it. It uses normative legal research with statutory, conceptual and case approaches, supported by secondary data. Confidentiality is protected in layers by Law No. 17 of 2023 on Health (Article 274(c) and Article 301), Minister of Health Regulation No. 24 of 2022 on Medical Records, and Law No. 27 of 2022 on Personal Data Protection (the PDP Law). The physiotherapy service standard (Minister of Health Regulation No. 65 of 2015) contains documentation forms but no confidentiality duty. Enforcement is fragmented: the administrative sanction in Regulation No. 24 of 2022 covers only the duty to operate an EMR, the data protection agency had not been formed on 16 September 2026, and by the authors' calculation the maximum fine in Article 67(1) of the PDP Law falls by 96.00% after the criminal-penalty adjustment. The study concludes that physiotherapists are bound by duties across the whole data cycle, but enforcement is incomplete and needs implementing regulations, a supervisory agency and clarity on the roles of the different supervisors.

***Keywords**:* health data confidentiality; electronic medical record; physiotherapy; personal data protection; physiotherapist

Dwi Selviany
Universitas Pembangunan Panca Budi Medan (UNPAP), Indonesia
e-mail: dwi.selviany80@gmail.com

Sutiarnoto, Muhammad Arif Sahlepi
e-mail: sutiarnoto@dosen.pancabudi.ac.id , arifsahlepi@dosen.pancabudi.ac.id
3rd International Conference Epicentrum of Economic Global Framework (ICEEGLOF)
Theme: Cross-Sector and Cross-Disciplinary Strategies for Achieving the SDGS
https://proceeding.pancabudi.ac.id/index.php/ICEEGLOF

Introduction

A physiotherapy medical record holds highly personal information: the patient's identity, assessment results, the physiotherapy diagnosis, the intervention plan and notes, and referrals [1], [2]. The physiotherapy service standard requires the whole physiotherapy process to be documented on the patient's medical record sheet [1]. Minister of Health Regulation No. 24 of 2022 on Medical Records (MoH Reg. 24/2022) requires every health facility, including the independent practice of a health worker, to operate an electronic medical record (EMR) by December 31, 2023 at the latest [2]. Law No. 27 of 2022 on Personal Data Protection (the PDP Law) places health data and information among specific personal data [3].

The group affected by these duties is small but dispersed. Statistics Indonesia (BPS) recorded 13,528 physical therapy personnel in 2023, or 0.90% of about 1.5 million health workers by the authors' calculation from figures published by GoodStats [4]. Under Law No. 17 of 2023 on Health (the Health Law), this group comprises physiotherapists, occupational therapists, speech therapists and acupuncturists [5], [6], so the number of physiotherapists is smaller than that figure. Physiotherapy is also delivered in independent practice and through home visits [7], [8], and in independent practice the operation of the EMR is the responsibility of the health worker concerned [2].

The risk is real. In May 2021, an alleged leak of data linked to BPJS Kesehatan drew public attention: the seller claimed to offer hundreds of millions of records, and the sample examined by the Ministry of Communication and Informatics contained 100,002 records. The report read mentions no sanction [9]. On July 30, 2026, the Ministry of Health, the Corruption Eradication Commission, the Ministry of Home Affairs, BPJS Kesehatan and the National Cyber and Crypto Agency signed a joint circular that sets an EMR based on the population identification number (NIK) and integrated with SATUSEHAT as the national guideline for hospitals [10].

Earlier studies of physiotherapy law mostly discuss the legal protection of physiotherapists and patients [8], [11] and the keeping of medical records [7]. Studies of patient data confidentiality discuss EMR in general [12] or online health applications [13]. In the sources reviewed, the authors found no study that maps a physiotherapist's confidentiality duties across the data cycle under the Health Law, Minister of Health Regulation (MoH Reg.) No. 24 of 2022 and the PDP Law together.

This article asks two questions. First, how is the confidentiality of patient health data protected in physiotherapy services? Second, what are the physiotherapist's legal duties in keeping patient health information confidential, especially in recording, storing and using the EMR? From the answers, the article also identifies gaps in enforcement and proposes steps to close them.

Literature Review

2.1 Health secrets, medical records and personal data

The Health Law requires medical and health personnel, in practice, to keep the patient's health secrets (Article 274(c)) and to make and keep notes or documents on examinations, care and procedures (letter d). Article 301(1) requires them to keep the patient's personal health secret, paragraph (2) allows disclosure for particular interests under Article 4(4), and paragraph (3) leaves further regulation to a government regulation [6]. Article 296 requires every medical and health worker providing individual care to make a medical record and to complete it promptly after the service ends. Article 297 states that the medical record document belongs to the health facility, that the patient has the right to access the information in it, and that the facility must keep the data secure, intact, confidential and available [6].

The PDP Law adds duties for the personal data controller: to have a basis for processing, with explicit valid consent as one of them (Article 20), to obtain consent in writing or in recorded form (Article 22), to protect and secure the data (Article 35), to keep it confidential

(Article 36), to prevent unauthorised access (Article 39(1)), and to give written notice within 3 x 24 hours when a failure of personal data protection occurs (Article 46(1)) [3]. Controllers, processors and related parties must adjust their processing within two years of the promulgation of the law (Article 74) [3].

2.2 Earlier studies on physiotherapy and data confidentiality

A sociological-juridical study of home-care physiotherapy in Semarang concluded that medical records were not kept well, with about 37.1% of physiotherapists not yet keeping a medical record [7]. An earlier study in the same city found that some independent physiotherapists did not obtain consent to treatment and did not keep medical records, in addition to licensing violations [11]. A study in Denpasar (2026) found that physiotherapists explain consent during home visits and give patients assessment sheets, and concluded that legal protection is needed; its abstract does not discuss confidentiality [8].

Indra et al. examined MoH Reg. 24/2022 and concluded that EMR data confidentiality is reasonably well protected and consistent across regulations, but that implementation has gaps, among them the status of electronic signatures, migration of paper records, procedures for disclosing medical information, and mechanisms for reporting data leaks. In their view, government access to the EMR does not yet meet the principle of legal protection for patients because the rules lack detail [12]. Tombokan et al. concluded that the confidentiality of patient data in electronic medical records on online health applications rests mainly on the PDP Law, and that misuse can be sanctioned under the PDP Law, the Electronic Information and Transactions Law and related regulations [13]. Neither study deals specifically with physiotherapy.

2.3 Legal politics, criminal policy and oversight

The analysis draws on studies by lecturers of Universitas Pembangunan Panca Budi. Five studies by Tanjung with co-authors form the main basis. In a critique of the omnibus method, Tanjung and Arminsyah argue that opaque process and thin public participation weaken legitimacy, and that broad government power to change regulations is a risk [14]. In a study of judicial oversight, Tanjung examines the Judicial Commission's supervision of judges and notes that other bodies also hold oversight powers [15]. In studies of cybercrime (with Adriani) and narcotics trafficking, he analyses penal and non-penal measures, and the narcotics study proposes an integrated approach of prevention, enforcement, therapy and rehabilitation [16], [17]. In a recent study with Arminsyah and Syam on the authority dualism between the National Sharia Arbitration Board (Basyarnas) and the sharia courts, they propose a model in which Basyarnas resolves sharia economic disputes through arbitration and the court supervises, legalises and enforces the awards, with synchronised regulation [18].

Studies by other lecturers in the same institution complete the framework. Suwarto, Sutiarnoto and Magda find that criminal law policy on digital crime in the era of artificial intelligence remains reactive, fragmented and rooted in classical thinking, which makes it hard to define offences, assign liability and prove crimes; they suggest harmonising norms, strengthening accountability models and integrating penal and non-penal policy [19]. Sinaga, Zarzani and Sahlepi, in a study of medical disputes between midwives and patients, find that the shift from litigation to non-litigation is not yet accompanied by norms on institutional roles and technical procedures, and that the structure and authority of the new disciplinary council are unclear [20]. Farhan, Sahlepi and Risdawati find that policies supporting the rights of patients with mental disorders to health services exist but are weakly applied [21]. Adrianto, Sumarno and Zarzani find a considerable gap between regulation and practice in the protection of health workers in remote areas, with weak coordination between agencies [22]. Mahruzar, Simarmata and Sahlepi find a normative conflict between general criminal law and a newer, more specific statute in the legal protection of doctors, and view criminal law as a last resort [23]. Zarzani, Ismaidar and Sihombing study corporate criminal liability and note that Law No.

32 of 2009 raises the threatened fine by one third when an offence is committed by or on behalf of a legal entity [24].

Research Method

This is normative legal research with statutory, conceptual and case approaches. The primary legal materials are Articles 4, 199, 274, 296, 297, 301, 304, 306 and 308 of the Health Law [6]; MoH Reg. 24/2022, read from the official text of the Ministry of Health (Articles 1 to 47) [2]; MoH Reg. 65/2015 on Physiotherapy Service Standards, read from the text in the BPK database [1]; Articles 4, 20, 22, 35, 36, 39, 46, 58, 59, 67, 68, 70 and 74 of the PDP Law [3]; Article 443 of the Criminal Code (KUHP) [25]; and Article II(5) of Law No. 1 of 2026 on Criminal Penalty Adjustment [26]. The secondary materials are journal articles, legal commentaries and press reports, including the studies by Panca Budi lecturers cited above. The secondary empirical data are the 2023 BPS figures as published by GoodStats, press reports of the alleged BPJS Kesehatan data leak (2021), press reports on the status of the data protection agency (September 16, 2026), and the Ministry of Health press release on the joint circular of July 30, 2026. The case approach uses the alleged BPJS Kesehatan leak as the only incident; the authors found no incident or decision involving physiotherapy specifically.

The analysis is descriptive and qualitative with three simple measures, all calculated by the authors. A percentage is the part divided by the total. The change in a fine is the fine after adjustment minus the original fine, divided by the original fine. The corporate fine is the individual fine multiplied by ten under Article 70(3).

The study has limitations. First, the Pasal.id page for Article 4 of the Health Law does not contain paragraph (1); the right to confidentiality (letter i) is inferred from the cross-reference in paragraph (4), and the paragraph number of Article 199 that lists the physical therapy group cannot be confirmed. Second, the authors did not find the article of Government Regulation No. 28 of 2024 that implements Article 301(3); the statement that the details of personal health secrets sit in the ministerial regulation and the PDP Law refers to the articles read. Third, Appendix I of Law No. 1 of 2026 was not included in the text read; the PDP Law fines after adjustment are read from one legal commentary [27] and cross-checked against the prison-term bands in Article II(5). Fourth, Articles 57 and 70 of the PDP Law could be read only in part on Pasal.id, so the corporate fine rule is read from a 2022 press report [28]. Fifth, the status of MoH Reg. 24/2022 against newer regulations was not checked against primary sources. Sixth, the BPS category includes occupational therapists, speech therapists and acupuncturists, so the number of physiotherapists is unknown. Seventh, the authors found no leak data, complaints or decisions specific to physiotherapy and could not access the Supreme Court Decision Directory; this reflects the search, not proof of absence. The alleged BPJS Kesehatan leak is an allegation as reported.

Results and Discussion

4.1 Protection of the confidentiality of patient health data

Table 1 maps the provisions that apply to physiotherapy patient data. The rules are spread over three levels, namely the statute, the ministerial regulation and the personal data protection statute, with the physiotherapy standard as the technical reference.

Table 1. Map of the rules on patient data confidentiality in physiotherapy services

Instrument and article	What the provision says	Meaning for physiotherapy
Health Law, Art. 4(1)(i) and (4)	Right to confidentiality of personal health data and information; disclosure for particular interests: a request by law enforcement, handling of an epidemic, extraordinary event or disaster, limited education and research, protection of the safety of others, health maintenance and treatment, the patient's own request, administrative needs, insurance or financing, and other interests under regulations [6]	The patient may demand confidentiality; the exceptions are limited and listed
Health Law, Art. 274(c)–(d) and Art. 301	Medical and health personnel must keep the patient's health secrets and make and keep notes; must keep the patient's personal health secret; details to be set by government regulation [6]	Basis of the physiotherapist's personal duty (physical therapy group, Art. 199)
Health Law, Arts. 296 and 297	A medical record must be made and promptly completed; the document belongs to the facility; the patient has a right of access; the facility must keep the data secure, intact, confidential and available [6]	Institutional duty on the facility where the physiotherapist works
MoH Reg. 24/2022, Arts. 3, 13, 20, 29–31, 45	EMR required in all facilities, including independent practice, by Dec. 31, 2023 at the latest; in independent practice responsibility lies with the health worker; storage on a certified server or cloud with backup in a different location; access rights to enter, correct and view; correction within 2 x 24 hours [2]	An independent physiotherapist bears the facility's duty and the personal duty at once
MoH Reg. 24/2022, Arts. 25–26, 32–39	Document belongs to the facility, content to the patient; confidentiality applies even after the patient's death; disclosure with the patient's consent, or without consent for law enforcement, ethics or discipline, medical audit, epidemic or disaster, education and research, and the safety of others, with the identity withheld; retention of at least 25 years from the last visit [2]	Detailed rules on who may disclose and how long to keep
PDP Law, Arts. 4, 20, 22, 35, 36, 39, 46	Health data is specific personal data; basis for processing and written or recorded consent; protection, confidentiality and prevention of unauthorised access; written notice within 3 x 24 hours [3]	Placed on the controller; a physiotherapy practice or facility may be a controller
MoH Reg. 65/2015, Appendix	The whole physiotherapy process is documented in the medical record; forms for assessment, referral in and out, clinical summary, intervention and monitoring, and consent to treatment; no confidentiality duty or retention period [1]	The profession's technical reference is silent on confidentiality; the general rules apply

Note: the third column is the authors' reading; letter (i) of Article 4(1) is inferred from the cross-reference in paragraph (4). Source: as cited in the table.

Four points can be noted. First, confidentiality is protected in three layers: the patient's rights and the personnel's duties in the Health Law, the duties of facilities and personnel in MoH Reg. 24/2022, and the data subject's rights and the controller's duties in the PDP Law. Second, the status of the medical record is worded differently: the Health Law states that the document belongs to the facility (Article 297(1)), while MoH Reg. 24/2022 states that the

document belongs to the facility and its contents to the patient (Article 25(1) and Article 26(1)) [2], [6]. In the authors' reading the two formulations do not conflict, because the facility controls the medium and the patient controls the content, and the PDP Law treats the patient as the data subject. Third, Article 301(3) leaves the details of personal health secrets to a government regulation, but the details of who may disclose, when, and with whose consent that the authors read sit in the ministerial regulation, MoH Reg. 24/2022 (Articles 34 to 36) [2]. Fourth, the physiotherapy service standard has six forms, namely assessment, referral in, referral out, clinical note or summary, intervention and monitoring, and consent to treatment, but it does not contain the word "secret" and states no retention period [1]. The professional technical reference is therefore silent on confidentiality, and physiotherapists must read it from the general rules.

4.2 The physiotherapist's legal duties across the data cycle

Table 2 arranges the physiotherapist's duties by stage of the data cycle: recording, storing, using and disclosing, and responding to a leak. The duties are personal and institutional at once. Articles 274 and 301 make the physiotherapist personally responsible for the patient's secret, while Article 297 and MoH Reg. 24/2022 place operation and security on the facility [2], [6]. In independent practice both fall on the same person, because responsibility for operating the EMR lies with the health worker concerned (Article 13(5)) [2].

Table 2. The physiotherapist's legal duties by stage of the data cycle

Stage	Duty and basis	Notes on application to physiotherapy
Recording	Make a medical record and complete it promptly (Health Law Art. 296(1) and (3)); clinical content is entered by the treating health worker with name, time and signature, and identity data at least the record number, name and NIK (MoH Reg. 24/2022 Arts. 13(3), 14(2), 16(2)); basis for processing and written or recorded consent (PDP Law Arts. 20 and 22); consent-to-treatment form (MoH Reg. 65/2015, Form 6) [1]–[3], [6]	A record that is not made cannot be protected; 37.1% of home-visit physiotherapists in Semarang had not made one [7]
Storing and securing	Keep the data secure, intact, confidential and available (Health Law Art. 297(3)); certified server or cloud with periodic backup in a different location (MoH Reg. 24/2022 Art. 20); access rights to enter, correct and view, with correction within 2 x 24 hours (Art. 30); retention of at least 25 years (Art. 39(1)); protect and prevent unauthorised access (PDP Law Arts. 35 and 39) [2], [3], [6]	In independent practice, operation is the physiotherapist's own responsibility (Art. 13(5)) [2]
Using and disclosing	Keep the secret (Health Law Arts. 274(c) and 301(1)); disclose only for the interests in Art. 4(4) [6]; with the patient's consent, or without consent for listed purposes with the identity withheld (MoH Reg. 24/2022 Arts. 34 and 35); confidentiality applies even after the patient's death (Art. 32(1)); consent given by the closest family or guardian if the patient lacks capacity (Art. 34(3)–(4)) [2]	Referrals use the referral-in and referral-out forms [1]; the EMR–SATUSEHAT integration is not accompanied by a statement on consent or confidentiality in the release read [10]
Responding to a leak	Written notice to the data subject and the agency within 3 x 24 hours (PDP Law Art. 46(1)) [3]	The agency concerned had not been formed on Sep. 16, 2026 [29]

Note: the third column is the authors' reading. Source: as cited in the table.

Table 2 shows that the first duty, recording, is a precondition for the others, because a medical record that is not made cannot be kept confidential. The finding that 37.1% of home-visit physiotherapists had not yet made a medical record [7] shows that this first stage is already a problem. At the storage stage, MoH Reg. 24/2022 sets technical details seldom found in statutes: storage on a certified server or cloud, periodic backups in a different location, separate access rights for entering, correcting and viewing, and a correction limit of 2 x 24 hours [2]. At

the disclosure stage, the rules distinguish disclosure with the patient's consent from disclosure without consent for listed purposes. If the patient conveys the content of the record to the public through the mass media, the facility may disclose the content as a right of reply (Article 38) [2]. The 3 x 24-hour breach notification duty in Article 46 of the PDP Law is addressed to the data subject and the data protection agency [3]; that agency has not yet been formed, as discussed below.

Two notes should be added. First, the duties in Articles 35, 36, 39 and 46 of the PDP Law fall on the personal data controller [3]. In the authors' reading, a physiotherapy practice or facility that determines the purposes and means of processing patient data is a controller, but the definition of controller in Article 1 was not read directly. Second, the Ministry of Health release on the joint circular of July 30, 2026 calls data a strategic state asset and says access must be secure, but contains no statement on patient consent or confidentiality rules [10]. The circular is addressed to hospitals, so its effect on independent physiotherapy practice is unclear.

4.3 Legal consequences and enforcement gaps

Table 3 maps the legal consequences of a breach of confidentiality. There are six routes: disciplinary, administrative under MoH Reg. 24/2022, administrative under the PDP Law, professional-secrecy crime, personal data crime, and civil. Each route has a gap in the articles read.

Table 3. Legal consequences of a breach of patient data confidentiality and their gaps

Route	Basis and consequence	Target	What is unclear
Disciplinary	A council formed by the Minister determines whether a disciplinary violation occurred (Art. 304); sanctions: written warning, compulsory education or training, temporary deactivation of the registration certificate (STR) and/or a recommendation to revoke the practice permit (SIP) (Art. 306) [6]	Physiotherapist	The articles read do not list the types of disciplinary violation; the council's authority is unclear [20]
Administrative (medical records)	Written reprimand and/or a recommendation to revoke or revocation of accreditation, only for a facility that does not operate an EMR (MoH Reg. 24/2022 Art. 42, referring to Art. 3(1)) [2]	Facility	A breach of confidentiality (Arts. 32–36) is not listed as a ground for sanction
Administrative (personal data)	PDP Law Art. 57; implementing agency under Arts. 58 and 59 [3]	Data controller and processor	Agency not formed on Sep. 16, 2026; administrative sanctions could not yet be applied effectively according to an expert [29]
Criminal (profession)	Criminal Code Art. 443: disclosing a secret that must be kept by reason of office, profession or duty; up to 1 year of imprisonment or a category III fine [25]	Person	Prosecuted on complaint where another's secret is involved; Pasal.id notes that Law 1/2026 has amended this provision, and the result was not read
Criminal (personal data)	PDP Law Arts. 67 and 68: imprisonment of up to 4 to 6 years and/or a fine; Art. 70: management, controllers, those who gave orders, beneficial owners and/or the corporation, with a corporate fine of up to 10 times [28]; after adjustment, a category IV fine (Art. 67) and category V (Art. 68) [26], [27]	Individuals and corporations	Elements of intent and a purpose of benefit; a leak caused by negligence is not automatically covered [3]

Route	Basis and consequence	Target	What is unclear
Civil	A civil claim for acts that harmed a patient in health services against medical or health personnel requires a council recommendation first; the recommendation is given within 14 working days (Art. 308(2), (4), (7)) [6]	Physiotherapist	Unclear whether disclosure of a secret is an act in health services; paragraph (9) exempts crimes unrelated to health services

Note: the last column is the authors' reading of the text read. Source: as cited in the table.

Three gaps stand out. First, the administrative sanction in MoH Reg. 24/2022 attaches only to a breach of Article 3(1), the duty to operate an EMR (Article 42) [2]. A breach of confidentiality (Articles 32 to 36) is not listed as a ground for sanction in that text. Second, the administrative sanctions of the PDP Law depend on a data protection agency formed by the President (Article 58) whose tasks include enforcing administrative sanctions and facilitating out-of-court dispute resolution (Article 59) [3]. On September 16, 2026, the agency had not been formed, its presidential regulation had not been issued, and according to an expert administrative sanctions could not yet be applied effectively, while criminal sanctions have applied since 2022 [29]. Third, the criminal route is narrow. Article 67(1) of the PDP Law requires intent, unlawfulness and a purpose of benefiting oneself or another that may harm the data subject [3], so in the authors' reading a leak caused by negligent security is not automatically covered. Article 443 of the Criminal Code can be prosecuted only on complaint where another person's secret is involved [25].

Figure 1 compares the maximum fines for an individual in the text of the PDP Law with their values after the criminal-penalty adjustment. The text of the law threatens fines of IDR 5 billion (Article 67(1)), IDR 4 billion (paragraph (2)), IDR 5 billion (paragraph (3)) and IDR 6 billion (Article 68) [28]. Article II(5) of Law No. 1 of 2026 converts the fine in a combined prison-and-fine threat according to the length of imprisonment: more than 3 to 5 years becomes category IV, and more than 5 to 8 years becomes category V [26]. With prison terms of 5, 4 and 5 years (Article 67) and 6 years (Article 68), a legal commentary dated September 29, 2026 gives category IV (IDR 200 million) and category V (IDR 500 million), with the prison terms unchanged [27]. By the authors' calculation, the maximum fines fall by 96.00%, 95.00%, 96.00% and 91.67%. Because a corporate fine may be up to 10 times the maximum fine (Article 70(3)) [28], by the authors' calculation the upper limit for a corporation falls from IDR 50, 40, 50 and 60 billion to IDR 2, 2, 2 and 5 billion; the latter figures have not been checked against Appendix I and the corporate provisions of Law No. 1 of 2026. For a physiotherapy clinic with legal-entity status this difference determines the size of the threat; for an independent physiotherapist, the individual fine applies.

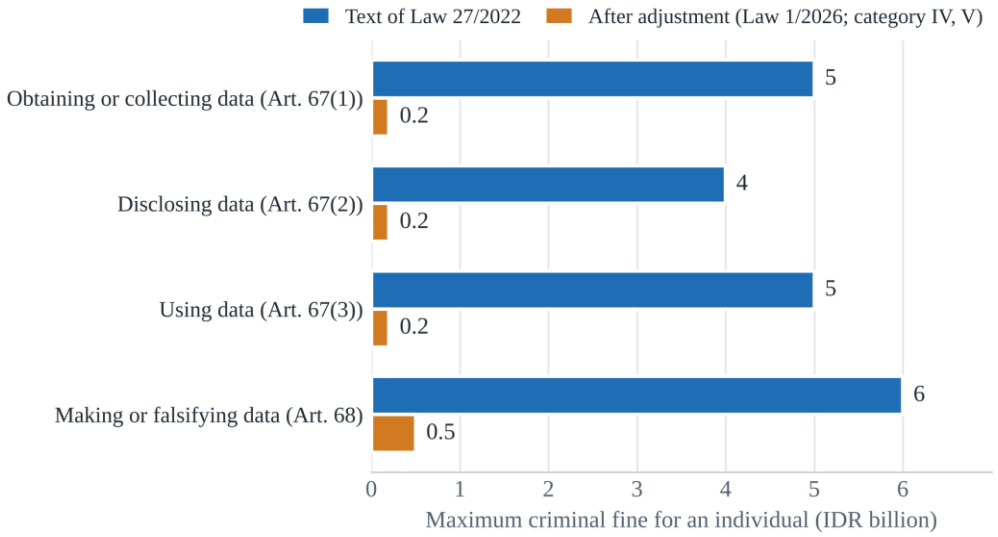


Figure 1. Maximum criminal fine for an individual in the PDP Law: text of the law and after the criminal-penalty adjustment (IDR billion). Source: [27], [28]; values after adjustment are read from one legal commentary and cross-checked against the band in Article II(5) [26].

Table 4 summarises the context indicators and the change in fines. Two indicators need careful reading. The figure of 37.1% comes from a single study in one city and concerns home-visit services [7], so it cannot be generalised. The figure of 100,002 is the number of records in the sample examined in the alleged BPJS Kesehatan leak, not the number of records leaked [9].

Table 4. Context indicators and the change in the maximum fines in Articles 67 and 68 of the PDP Law

Indicator	Value	Source
Health workers by BPS category, 2023 (sum of categories)	1,499,959	Calculated; [4]
Physical therapy personnel, 2023	13,528 (0.90%)	[4]
Deadline for EMR in all facilities	Dec. 31, 2023	[2]
Retention period for medical records	at least 25 years	[2]
Limit for correction of data by the treating worker	2 x 24 hours	[2]
Limit for notice of a failure of data protection	3 x 24 hours	[3]
Adjustment period under the PDP Law	2 years (ended Oct. 2024)	[3], [29]
Home-visit physiotherapists in Semarang who had not made a medical record	37.1%	[7]
Sample records in the alleged BPJS Kesehatan leak, 2021	100,002	[9]
Art. 67(1): IDR 5 billion to IDR 200 million	−96.00%	Calculated; [27]
Art. 67(2): IDR 4 billion to IDR 200 million	−95.00%	Calculated; [27]
Art. 67(3): IDR 5 billion to IDR 200 million	−96.00%	Calculated; [27]
Art. 68: IDR 6 billion to IDR 500 million	−91.67%	Calculated; [27]

Note: percentages calculated by the authors. The fine values after adjustment are read from one legal commentary and were not checked against Appendix I of Law No. 1 of 2026.

4.4 A legal-politics perspective

The findings can be read through Tanjung's work. Tanjung and Arminsyah warn that broad government power to change regulations is a risk to legitimacy [14]. Here, the Health Law only says that the details of personal health secrets are set by government regulation (Article 301(3)) [6], while the details the authors read sit in a ministerial regulation [2]. In the authors' reading, the rules that concern patient rights sit at a level below the government regulation, and the physiotherapy standard that guides the profession does not contain them [1].

Tanjung's study of judicial oversight notes that supervision is divided among several bodies [15]. A similar pattern appears here: the disciplinary council (Article 304 of the Health Law), the Director General for administrative sanctions on medical records (Article 42 of MoH Reg. 24/2022), the data protection agency (Articles 58 and 59 of the PDP Law), the Ministry of Communication and Digital Affairs for electronic system operators under Government Regulation No. 71 of 2019 [29], and the police and courts for crimes. The articles read do not say which body receives a complaint from a physiotherapy patient or how these bodies share information. The finding of Sinaga, Zarzani and Sahlepi on unclear institutional roles and disciplinary council authority [20] is consistent with this.

Tanjung and Adriani analyse penal and non-penal measures against cybercrime, and the narcotics study proposes an integrated approach [16], [17]; Suwarto, Sutiarnoto and Magda suggest integrating penal and non-penal policy for digital crime [19]. In health data, what works today is the penal route, because administrative sanctions wait for the agency [29], yet the penal route is narrow and its sanctions are falling. The view of criminal law as a last resort [23] supports a non-penal route that works first, namely professional standards, access control, training and administrative sanctions. The relationship between Article 443 of the Criminal Code and Article 67 of the PDP Law is not discussed in the sources read; the two differ in elements, namely disclosure of a secret by reason of profession and unlawful obtaining or disclosure of data.

The model of Tanjung, Arminsyah and Syam, in which an out-of-court body resolves the dispute while the court supervises, legalises and enforces the result, with synchronised regulation [18], fits the institutional design of the PDP Law. The PDP Law tasks the data protection agency with facilitating out-of-court dispute resolution (Article 59) [3], but the agency does not yet exist [29]. Applying that model to disputes over physiotherapy patient data is the authors' proposal, not a finding of that study.

Finally, Zarzani et al. note a one-third increase in fines for legal entities in Law No. 32 of 2009 [24], while the PDP Law uses a multiple of ten [28]; in the authors' reading, the corporate fine formula is not uniform across statutes. The finding of Adrianto et al. on the gap between regulation and practice [22] and the finding of Farhan et al. that supportive policies exist but are weakly applied [21] are consistent with the 37.1% figure: written duties have not yet become practice.

Recommendations

Five steps follow from this analysis. First, physiotherapists and practice operators need written confidentiality procedures: timely record-making, role-based access, written or recorded consent to data processing built into the consent-to-treatment form, backup and retention, and a breach notification procedure within 3 x 24 hours. Second, professional organisations and educators need to train physiotherapists, including those in independent practice and home visits, and administrative staff in these duties. Third, the government needs to update MoH Reg. 65/2015 to include a confidentiality duty and a retention period, clarify the government regulation that implements Article 301(3), and extend the grounds for administrative sanctions in MoH Reg. 24/2022 to breaches of confidentiality. Fourth, the government needs to form the data protection agency and set its division of powers with the disciplinary council and the Ministry of Health, including a complaint channel for patients. Fifth, it needs to be clarified whether disclosure of a health secret requires a council recommendation before investigation or suit (Article 308), a statement on consent and confidentiality is needed in the EMR–SATUSEHAT integration, and leak data specific to physiotherapy are needed.

Conclusion

First, the confidentiality of physiotherapy patients' health data is protected in layers: rights and duties in the Health Law (Articles 4, 274, 296, 297, 301), duties to operate, store and disclose medical records in MoH Reg. 24/2022, and the controller's duties in the PDP Law.

The physiotherapy service standard (MoH Reg. 65/2015) requires documentation but contains no confidentiality duty or retention period.

Second, the physiotherapist, as a health worker in the physical therapy group, must make a medical record, keep the patient's personal health secret, and disclose data only for permitted purposes. Where the physiotherapist is a controller, he or she must also secure the data and report a leak within 3 x 24 hours. In independent practice, responsibility for operating the EMR lies with the physiotherapist. The recording duty is not met by some practitioners, 37.1% in one study in Semarang.

Third, enforcement is incomplete. The administrative sanction in MoH Reg. 24/2022 covers only the duty to operate an EMR, the data protection agency had not been formed on September 16, 2026, and by the authors' calculation the maximum PDP Law fine for an individual falls by between 91.67% and 96.00% after the criminal-penalty adjustment. The authors recommend confidentiality procedures at the practice level, training, an update of the physiotherapy standard, formation of the agency, and clarity on the roles of the different supervisors. Further research should read Appendix I of Law No. 1 of 2026 and the implementing regulations of the Health Law in full, trace court decisions, and collect leak data specific to physiotherapy.

References

[1] Regulation of the Minister of Health of the Republic of Indonesia No. 65 of 2015 on Physiotherapy Service Standards, State Gazette of the Republic of Indonesia Year 2015 No. 1662, 2015. [Online]. Available: https://peraturan.bpk.go.id/Download/107456/Permenkes%20Nomor%2065%20Tahun%202015.pdf. [Accessed: Oct. 29, 2026]

[2] Regulation of the Minister of Health of the Republic of Indonesia No. 24 of 2022 on Medical Records, 2022. [Online]. Available: https://jdih.kemkes.go.id/common/dokumen/2022permenkes024.pdf. [Accessed: Oct. 29, 2026]

[3] "Articles 4, 20, 22, 35, 36, 39, 46, 58, 59, 67, 68, 70 and 74 of Law No. 27 of 2022 on Personal Data Protection," *Pasal.id*. [Online]. Available: https://pasal.id/peraturan/uu/uu-no-27-tahun-2022 (and /pasal-67, /pasal-70). [Accessed: Oct. 29, 2026]

[4] Agi, "Perawat dominasi tenaga kesehatan Indonesia, tenaga medis hanya 12,25% [Nurses dominate Indonesia's health workers, medical personnel only 12.25%]," *GoodStats*, Oct. 25, 2024. [Online]. Available: https://data.goodstats.id/statistic/perawat-dominasi-tenaga-kesehatan-indonesia-tenaga-medis-hanya-1225-U1hqe. [Accessed: Oct. 29, 2026]

[5] Law of the Republic of Indonesia No. 17 of 2023 on Health, 2023.

[6] "Articles 4, 199, 274, 296, 297, 301, 304, 306 and 308 of Law No. 17 of 2023 on Health," *Pasal.id*. [Online]. Available: https://pasal.id/peraturan/uu/uu-no-17-tahun-2023/pasal-301 (and /pasal-4, /pasal-199, /pasal-274, /pasal-296, /pasal-297, /pasal-304, /pasal-306, /pasal-308). [Accessed: Oct. 29, 2026]

[7] Kuswardani, "Implementation of medical records in physiotherapy services home care in Semarang City," *Al-Manhaj J. Huk. Pranata Sos. Islam*, vol. 6, no. 1, pp. 51–64, 2024, doi: 10.37680/almanhaj.v6i1.4342.

[8] A. A. S. N. Indradewi and R. M. Zulkarnain, "Perlindungan hukum terhadap fisioterapis dalam pelayanan fisioterapi mandiri di Kota Denpasar [Legal protection of physiotherapists in independent physiotherapy services in Denpasar City]," *Kerta Dyatmika*, vol. 23, no. 1, pp. 38–48, Mar. 2026. [Online]. Available: https://ejournal.undwi.ac.id/kertadyatmika/article/view/1807. [Accessed: Oct. 29, 2026]

[9] A. Sahbani, "Kebocoran data pribadi peringatan bagi ketahanan siber [Personal data leaks a warning for cyber resilience]," *Hukumonline*, May 24, 2021. [Online]. Available: https://www.hukumonline.com/berita/a/kebocoran-data-pribadi-peringatan-bagi-ketahanan-siber-lt60aaadc386b73?page=all. [Accessed: Oct. 29, 2026]

[10] "Kemenkes perkuat tata kelola klaim JKN melalui integrasi rekam medis elektronik dengan SATUSEHAT [Ministry of Health strengthens JKN claims governance through integration of electronic medical records with SATUSEHAT]," Secretariat General, Ministry of Health of the Republic of Indonesia, Jul. 30, 2026. [Online]. Available: https://setjen.kemkes.go.id/news/kemenkes-perkuat-tata-kelola-klaim-jkn-melalui-integrasi-rekam-medis-elektronik-dengan-satusehat. [Accessed: Oct. 29, 2026]

[11] Kuswardani, A. J. Purwoko, and D. B. Wibowo, "Pelaksanaan perlindungan hukum terhadap pasien sebagai konsumen jasa dan fisioterapis dalam pelayanan fisioterapi mandiri di Kota Semarang [Implementation of legal protection for patients as service consumers and physiotherapists in independent physiotherapy services in Semarang City]," *J. Fisioter. Rehabil.*, vol. 2, no. 2, pp. 79–103, 2018, doi: 10.33660/jfrwhs.v2i2.25.

[12] Indra, T. N. Dewi, and D. B. Wibowo, "Perlindungan kerahasiaan data pasien vs kewajiban membuka akses rekam medis elektronik [Protection of patient data confidentiality vs the obligation to open access to electronic medical records]," *SOEPRA J. Huk. Kesehat.*, vol. 10, no. 1, pp. 97–117, Jun. 2024, doi: 10.24167/shk.v10i1.11542.

[13] C. D. Tombokan, H. Y. Rumengan, and R. Y. J. Kaligis, "Perlindungan hukum terhadap kerahasiaan data pasien dalam aplikasi layanan kesehatan online yang disalahgunakan [Legal protection of the confidentiality of patient data in misused online health service applications]," *Lex Privatum*, vol. 14, no. 4, Dec. 2024. [Online]. Available: https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/download/59386/48230. [Accessed: Oct. 29, 2026]

[14] I. U. Tanjung and Arminsyah, "Kritik terhadap implementasi Omnibus Law dalam sistem hukum Indonesia: Analisis dari perspektif hukum tata negara [Criticism of the implementation of the Omnibus Law in the Indonesian legal system: An analysis from a constitutional law perspective]," *Juris Sinergi J.*, vol. 1, no. 1, pp. 1–8, May 2024, doi: 10.70321/jsj.v1i1.11.

[15] I. U. Tanjung, "Eksistensi Komisi Yudisial dalam pengawasan hakim [The existence of the Judicial Commission in the supervision of judges]," *Al-Fikru*, vol. 15, no. 2, pp. 65–77, 2021, doi: 10.51672/alfikru.v15i2.52.

[16] I. U. Tanjung and E. N. Adriani, "Politik hukum terhadap penanggulangan kejahatan dunia maya [Legal politics on combating cybercrime]," *Judge J. Huk.*, vol. 3, no. 1, pp. 1–8, 2023, doi: 10.54209/judge.v3i01.371.

[17] I. U. Tanjung, "Strategi pemberantasan mafia narkoba (pendekatan politik hukum) [Strategies for combating the narcotics mafia: A legal-politics approach]," *Judge J. Huk.*, vol. 3, no. 1, pp. 10–19, 2023, doi: 10.54209/judge.v3i01.372.

[18] Arminsyah, I. U. Tanjung, and S. A. Syam, "Resolving authority dualism between National Sharia Arbitration Board and Sharia Courts through maslahah," *As-Siyasi J. Const. Law*, vol. 6, no. 1, pp. 401–416, 2026, doi: 10.24042/as-siyasi.v61.31910.

[19] Suwarto, Sutiarnoto, and M. Magda, "Reconstruction of criminal law policy in tackling digital-based crime in the era of artificial intelligence," *Ipso Jure*, vol. 2, no. 12, pp. 85–94, 2025, doi: 10.62872/bjc35s29.

[20] T. A. P. Sinaga, R. Zarzani, and M. A. Sahlepi, "Model penyelesaian sengketa medis antara bidan dan pasien dalam sistem hukum kesehatan nasional [A model for resolving medical disputes between midwives and patients in the national health legal system]," *Blantika Multidiscip. J.*, vol. 4, no. 5, 2026, doi: 10.57096/blantika.v4i5.493.

[21] Farhan, M. A. Sahlepi, and I. Risdawati, "Analysis of the implementation of the rights of patients with mental disorders to access health services in hospitals Prof. Dr. Muhammad Ildrem North Sumatra," *Equivalent J. Econ. Account. Manag.*, vol. 4, no. 2, pp. 2438–2450, 2026, doi: 10.61994/equivalent.v4i2.1934.

[22] I. Adrianto, S. Sumarno, and T. R. Zarzani, "Legal protection for health workers working in remote areas: Research study in Kapuas Hulu Regency," *Int. J. Sociol. Law*, vol. 1, no. 4, pp. 176–185, 2024, doi: 10.62951/ijsl.v1i4.187.

[23] R. Mahruzar, M. Simarmata, and M. A. Sahlepi, "Legal protection for doctors providing health services: A study of Decision Number 365 K/Pid/2012," *J. Multidisiplin Indones.*, vol. 5, no. 4, pp. 172–186, 2026, doi: 10.58344/jmi.v5i4.2672.

[24] T. R. Zarzani, I. Ismaidar, and M. Sihombing, "Corporate criminal liability in environmental pollution crimes," *Int. J. Sociol. Law*, vol. 1, no. 3, pp. 31–40, 2024, doi: 10.62951/ijsl.v1i3.101.

[25] "Article 443 of Law No. 1 of 2023 on the Criminal Code," *Pasal.id*. [Online]. Available: https://pasal.id/peraturan/uu/uu-no-1-tahun-2023/pasal-443. [Accessed: Oct. 29, 2026]

[26] Law of the Republic of Indonesia No. 1 of 2026 on Criminal Penalty Adjustment, 2026. [Online]. Available: https://jdih.kemenkoinfra.go.id/dokumen/file/uu/2026/uu-nomor-1-tahun-2026.pdf. [Accessed: Oct. 29, 2026]

[27] M. R. Nugraha, "Jenis tindak pidana pelindungan data pribadi [Types of crimes in personal data protection]," *Hukumonline*, Sep. 29, 2026 (updated Sep. 30, 2026). [Online]. Available: https://www.hukumonline.com/klinik/a/jenis-tindak-pidana-pelindungan-data-pribadi-lt694a430534712/. [Accessed: Oct. 29, 2026]

[28] A. T. Haryanto, "Langgar dan bocorkan data pribadi, korporasi bisa dibubarkan! [Violate and leak personal data, corporations can be dissolved!]," *detikInet*, Sep. 20, 2022. [Online]. Available: https://inet.detik.com/law-and-policy/d-6302834/langgar-dan-bocorkan-data-pribadi-korporasi-bisa-dibubarkan. [Accessed: Oct. 29, 2026]

[29] I. Rakhmayanti, "Lembaga perlindungan data belum ada di RI, padahal aturannya sudah ada [Data protection agency does not yet exist in Indonesia although the rules do]," *CNBC Indonesia*, Sep. 16, 2026. [Online]. Available: https://www.cnbcindonesia.com/tech/20260916115609-37-768328/lembaga-perlindungan-data-belum-ada-di-ri-padahal-aturannya-sudah-ada. [Accessed: Oct. 29, 2026]