

Legal Protection of Anesthesia Practitioners in the Digitalization of SIPPA through SATUSEHAT

I Made Oktavian Dwi Chandra^{1*}, I Gusti Ayu Putri Kartika²

^{1,2} Magister Hukum Kesehatan, Universitas Udayana

*Correspondence: oktaviand45@gmail.com

Received: 1 August 2026

Accepted: 07 September 2026

Published: 20 September 2026

Abstrak

Digitalisasi sistem perizinan tenaga kesehatan merupakan bagian dari transformasi tata kelola kesehatan nasional yang bertujuan meningkatkan efisiensi, integrasi data, dan transparansi pelayanan. Salah satu bentuk penerapannya adalah proses penerbitan Surat Izin Praktik Penata Anestesi (SIPPA) melalui sistem digital yang terintegrasi dengan platform SATUSEHAT. Namun, ketergantungan terhadap sistem digital juga menimbulkan persoalan hukum, terutama berkaitan dengan kepastian hukum dan perlindungan data pribadi tenaga penata anestesi. Penelitian ini bertujuan menganalisis ketentuan hukum yang mengatur digitalisasi SIPPA setelah berlakunya Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan serta menganalisis perlindungan hukum terhadap data pribadi tenaga penata anestesi dalam proses penerbitan SIP melalui sistem digital. Penelitian menggunakan metode hukum normatif dengan pendekatan peraturan perundang-undangan dan pendekatan konseptual. Bahan hukum dianalisis secara kualitatif dengan menelaah keterkaitan antara UU Kesehatan, UU Pelindungan Data Pribadi, PP Nomor 28 Tahun 2024, dan Permenkes Nomor 13 Tahun 2025. Hasil penelitian menunjukkan bahwa digitalisasi SIP memiliki dasar hukum yang cukup, tetapi pelaksanaannya harus memperhatikan pembagian kewenangan penerbitan SIP, keamanan dan akurasi data, serta mekanisme penyelesaian ketika terjadi kegagalan sistem. Pelindungan hukum bagi penata anestesi tidak hanya berkaitan dengan legalitas praktik, tetapi juga dengan hak atas data pribadi dan kepastian prosedur ketika terjadi gangguan atau kesalahan dalam sistem digital.

Kata kunci: perlindungan hukum; penata anestesi; SIPPA; digitalisasi perizinan; SATUSEHAT; data pribadi.

Abstract

The digitalization of health workforce licensing is part of a broader transformation of health governance that places information systems at the centre of professional administrative processes. One of its implementations is the issuance of the Anesthesia Practitioner Practice License (Surat Izin Praktik Penata Anestesi/SIPPA) through a digital system integrated with the SATUSEHAT platform. Reliance on digital systems, however, also raises legal concerns, particularly concerning legal certainty and the protection of anesthesia practitioners' personal data. This study examines the legal framework governing the digitalization of SIPPA following the enactment of Law Number 17 of 2023 on Health and analyses the legal protection of personal data during the digital licensing process. The study employs normative juridical research using statutory and conceptual approaches. Legal materials are analysed qualitatively by examining the relationship among the Health Law, the Personal Data Protection

Law, Government Regulation Number 28 of 2024, and Minister of Health Regulation Number 13 of 2025. The findings indicate that digital SIP licensing has a sufficient legal basis, but its implementation must address licensing authority, data security and accuracy, and remedies for system failures. Legal protection for anesthesia practitioners therefore concerns not only the legality of professional practice, but also personal data rights and clear procedures when errors or disruptions occur in the digital licensing system.

Keywords: *legal protection; anesthesia practitioners; SIPPA; digital licensing; SATUSEHAT; personal data.*

INTRODUCTION

In this article, “anesthesia practitioner” is used as the English rendering of the regulated Indonesian profession *Penata Anestesi*. The term is used for readability and does not imply the creation of a profession different from the category recognized in Indonesian health regulation. Anesthesia practitioners play an important role in anesthesia services and are subject to professional competency standards, including the national Professional Standards for Anesthesia Practitioners.¹

The licensing requirement should not be understood merely as an administrative formality. A practice licence determines whether a health professional may lawfully provide services in a particular setting. Research on anesthesia practice has shown that STRPA and SIPPA are important instruments for demonstrating professional eligibility and regulating perioperative anesthesia services. At the same time, studies concerning practice without a licence show that the absence of SIP can expose practitioners and health facilities to legal consequences.²

The development of digital government services has changed the way professional licensing is administered. Law Number 17 of 2023 on Health places health administration within a framework that increasingly uses information technology and integrated health information systems. This direction is consistent with the broader legal recognition of electronic information and transactions and with the policy objective of integrating health workforce data. Digitalization can reduce repetitive administration, improve verification, and make licensing status easier to monitor.³

The move to digital licensing, however, changes the nature of the legal risks involved. Under a conventional system, an applicant can usually retain physical documents and obtain direct administrative evidence of submission. In a digital system, the validity of the process may depend on electronic records, authentication,

¹A. Wahyudi, D. Nurhidayati, and R. Setiawan, “Implementasi KMK Nomor HK.01.07/MENKES/722/2020 tentang Standar Profesi *Penata Anestesi* di Indonesia,” *Jurnal Kebijakan Kesehatan Indonesia* (2023).

²Rina Kumala, Hendra Suherman, and Deaf Wahyuni, “Efektivitas Regulasi Penyelenggaraan Praktik *Penata Anestesi* dengan STRPA dan SIPPA dalam Pelayanan Anestesiologi Perioperatif,” *Jurnal Kebijakan Kesehatan Indonesia* 12, no. 1 (2023): 22–26, <https://doi.org/10.22146/jkki.81459>.

³Aditya Dwi Purwaningsih and Purnawan Junadi, “Kebijakan Penerbitan Surat Tanda Registrasi Bagi Tenaga Medis dan Tenaga Kesehatan: Literature Review,” *Jurnal Ners* 9, no. 4 (2025): 7898–7904, <https://doi.org/10.31004/jn.v9i4.51130>.

database synchronization, and the availability of the platform. If an application is delayed or incorrectly recorded because of a technical or administrative problem, the practitioner may face consequences even though the substantive requirements have been fulfilled. This creates a legal-certainty issue that cannot be solved by technology alone.⁴

A second legal issue concerns personal data. The digital licensing process requires the processing of information relating to the identity and professional status of anesthesia practitioners. Such information may include identity numbers, professional registration numbers, educational qualifications, certification, practice information, and other data used for verification. Once these data are processed electronically and integrated into a wider health information environment, the risks are not limited to simple administrative errors. Unauthorised access, excessive disclosure, inaccurate records, data loss, and security breaches may affect the professional and personal interests of the data subject.

Digital SIPPA sits at the intersection of three legal domains that must be read together. First, health-professional licensing law determines the substantive authority to practise and the institution competent to issue a practice licence. Second, digital-administration rules govern the electronic workflow, data exchange, verification, audit trail, and attribution of administrative acts. Third, personal-data law governs the lawful basis, purpose, accuracy, security, correction, and breach response for data processed in that workflow. The rights of an applicant and the responsibilities of institutions can be identified only by separating these three layers and then reconnecting them in the same licensing process.

Previous studies can be grouped into three strands. One examines the professional status of *Penata Anestesi* and the legal function of STRPA/SIPPA; a second addresses digital registration and health-workforce administration; and a third examines personal-data protection in SATUSEHAT and digital health systems.⁵ These studies establish important components of the legal framework but do not fully map the consequences that arise when an integrated digital system affects the validity, timeliness, or evidentiary proof of a professional licence.

The specific research gap therefore concerns the legal interface among licensing authority, digital-system dependence, and data protection. This article contributes an institutional-responsibility map and an evaluation matrix covering authority, lawful basis, security, correction, incident response, remedies, audit trails, and contingency. It does not claim that downtime, data mismatch, non-issuance, or data breaches occur at a particular frequency; where such scenarios are discussed without an official incident record, they are treated as projected legal risks derived from the structure of mandatory digital administration.

The regulatory chain comprises Law Number 17 of 2023 on Health, Government Regulation Number 28 of 2024, and Minister of Health Regulation Number 13 of 2025 on the Management of Health Human Resources, together with

⁴Gunawan Wahyudiono, Joko Ismono, and Nuryanto A. Daim, "Perlindungan Hukum Tenaga Kesehatan (Penata Anestesi) Setelah Terbitnya Undang-Undang Kesehatan Nomor 17 Tahun 2023," *Law and Humanity* 2, no. 1 (2024): 1–17, <https://doi.org/10.37504/lh.v2i1.605>.

⁵Rahmadi Indra Tektana, Fendi Setyawan, and Frederica Prima, "Kepastian Hukum Pemilik Data Pribadi Dalam Aplikasi Satu Sehat," *Jurnal Legislasi Indonesia* 20, no. 1 (2023): 28–41, <https://doi.org/10.54629/jli.v20i1.996>.

Law Number 27 of 2022 on Personal Data Protection. SATUSEHAT SDM functions as an integrated health-workforce data platform and is connected to professional-licensing services; the platform interface should nevertheless be distinguished from the legally competent authority that attributes and issues the administrative licensing decision.

Legal protection must therefore follow the entire chain. Preventive protection concerns clear competence, lawful processing, data minimization, security, correction, traceability, and a contingency route before a dispute occurs. Repressive protection concerns restoration of the practitioner's legal position after an error or incident, including complaints, correction, administrative review where available, incident notification, evidence preservation, and accountability. The digital platform is a means of administration, not an independent source of licensing authority.

This study therefore examines three related questions. First, what legal provisions govern the digitalization of SIPPA after Law Number 17 of 2023? Second, how is the personal data of anesthesia practitioners protected during SIPPA issuance through SATUSEHAT? Third, what legal implications arise from system disruption, inaccurate data, and personal-data breaches in the digital licensing process?

The study is expected to contribute to health law scholarship by connecting professional licensing, digital administration, and personal-data protection. It also seeks to clarify the responsibilities of government institutions and the position of anesthesia practitioners as both licensing applicants and data subjects. The analysis is directed toward a legal framework that preserves administrative efficiency without weakening legal certainty and professional protection.

RESEARCH METHOD

This study uses a normative juridical research method. The method is appropriate because the central issues concern the interpretation and application of legal norms governing professional licensing, health information systems, digital administration, and personal data protection. The research does not measure the experiences of anesthesia practitioners through surveys or interviews. Instead, it examines the legal framework and the relationship among the relevant rules in order to determine the extent to which those rules provide legal certainty and protection during the digital issuance of SIPPA.

The statutory approach examines Law Number 17 of 2023 on Health, Law Number 27 of 2022 on Personal Data Protection, Government Regulation Number 28 of 2024, Minister of Health Regulation Number 13 of 2025 on the Management of Health Human Resources, and relevant professional instruments including the Minister of Health Decree on Professional Standards for Anesthesia Practitioners. Potential overlap is assessed through systematic interpretation, the hierarchy of norms, and *lex specialis* reasoning where a sector-specific health rule and the general personal-data framework regulate different aspects of the same processing activity.

The conceptual approach is used to analyse legal protection and legal certainty in the context of digital licensing. Legal protection is examined through preventive and repressive dimensions. Preventive protection concerns the measures that should exist before a violation or dispute occurs, including clear procedures, lawful data processing, security controls, and opportunities to correct information.

Repressive protection concerns the mechanisms available after a problem has occurred, such as complaints, correction, recovery, notification of a data breach, and legal accountability. Legal certainty is examined through the clarity of norms, distribution of authority, consistency of procedures, and availability of remedies.⁶

Primary legal materials consist of legislation and authoritative policy documents governing licensing, health information systems, and personal data. Secondary materials consist of peer-reviewed legal and health-administration literature published principally from 2020 to 2026, supplemented by older doctrinal works on legal protection and legal certainty. Materials were identified through official legal databases and institutional websites and through scholarly searches using combinations of the terms “Penata Anestesi,” “SIPPA,” “SATUSEHAT,” “health professional licensing,” “personal data protection,” “digital health,” and “legal certainty.” Sources were selected for direct relevance to the legal issues, currentness of the applicable regulatory framework, and traceability of publication data.

The analysis proceeded in five stages. First, the study mapped the legal status of SIPPA and the allocation of authority among the health-workforce data platform, the competent licensing authority, health facilities, and source-data institutions. Second, it mapped rules on electronic administration and integrated health information systems. Third, it classified the data processed in licensing as general identity data, professional/administrative data, and data that may fall within specific personal-data categories when health or biometric information is processed. Fourth, it tested projected legal risks against the positive-law requirements on authority, lawful basis, security, accuracy, correction, incident response, auditability, and remedies. Fifth, it assessed gaps through the concepts of preventive and repressive legal protection and legal certainty. Because the study contains no interviews, user observation, or incident dataset, it cannot determine implementation effectiveness, user experience, or the frequency of system failures.

RESULTS AND DISCUSSION

Legal Provisions Governing Digital SIPPA after Law Number 17 of 2023

The legal status of SIPPA must first be understood within the general framework of health-professional licensing. A practice licence is not merely an administrative registration; it is the formal administrative basis through which a health professional demonstrates authority to practise in the relevant setting. For anesthesia practitioners, whose work occurs in a high-risk clinical environment, the validity and traceability of the practice licence are therefore closely connected to professional legal certainty.

Law Number 17 of 2023 and its implementing regulations place health administration within an increasingly integrated digital-information framework. This supports electronic licensing because verified professional data can be reused across connected administrative processes. Digital integration may reduce repetitive submissions and improve verification, but those advantages do not change the requirement that an administrative decision be attributable to a legally competent authority.

⁶Satjipto Rahardjo, *Ilmu Hukum* (Bandung: Citra Aditya Bakti, 2000).

Government Regulation Number 28 of 2024 provides a more operational framework for health professional licensing and the implementation of the Health Law. It regulates licensing requirements and the use of information systems in the health sector. The regulation is important because it connects the general statutory framework with administrative implementation. At the same time, the digital platform used to process an application should be distinguished from the government authority legally responsible for the licensing decision.⁷

The distinction between platform operation and administrative authority has concrete consequences. SATUSEHAT SDMK may receive, store, display, and exchange professional data, while the formal licensing act remains attributable to the competent licensing authority designated by applicable law and implementing regulation. A system-generated status, therefore, should be legally traceable to the authority responsible for the decision. If a technical error, synchronization failure, or inaccurate automated rule affects the outcome, the applicant should have a route to establish the original submission and obtain correction without being treated as professionally non-compliant merely because of an error outside the applicant's control.

Minister of Health Regulation Number 13 of 2025 reinforces the movement toward electronic management of health human resources. For types of SIP issued through the national mechanism, the regulation provides an electronic process involving submission, verification, and issuance through an integrated information system. Although not every provision is directed specifically at anesthesia practitioners, the regulation illustrates the broader policy direction in which health professional administration is increasingly conducted electronically. SIPPA should therefore be interpreted within this wider system rather than as a separate licensing instrument.

The digitalization of SIPPA offers several administrative advantages. Electronic submission can reduce physical document handling and shorten verification time. Integrated data can reduce duplication because verified professional information can be reused for relevant administrative processes. A 1148epractises1148 information environment can also support government oversight and make licensing status easier to verify. These benefits are consistent with the objectives of efficient and transparent health administration.

Efficiency, however, cannot be separated from data accuracy. A digital system is only as reliable as the information stored and exchanged within it. If a registration number, educational record, practice location, or other licensing information is inaccurate, the system may generate an incorrect administrative outcome. When databases are integrated, an error may also be transferred automatically between systems. Digital integration therefore requires validation, traceability, and a practical mechanism for correction.

The legal consequences of an inaccurate record should not automatically be imposed on the applicant. A professional who has submitted correct information should have an opportunity to demonstrate that an error arose during verification or integration. Legal certainty requires a procedure that distinguishes applicant

⁷Indonesia, Government Regulation Number 28 of 2024 concerning the Implementing Regulation of Law Number 17 of 2023 on Health, State Gazette of the Republic of Indonesia Year 2024 Number 135.

error from administrative or system error and preserves evidence of the original submission. Without such a mechanism, digital efficiency may shift the burden of administrative failure to the person who depends on the system.

System interruption is analysed here as a projected legal risk rather than as a documented claim about the frequency of SATUSEHAT failure. The relevance of the scenario arises from the legal dependence created by electronic processing: if a prescribed digital channel is unavailable, a practitioner may be unable to submit, verify, or prove timely compliance. The legally important question is therefore whether the regulatory and operational framework preserves evidence of attempted compliance and supplies a fallback route when the mandated channel cannot be used.

From the perspective of legal certainty, the digital platform should provide clear information about the beginning and end of each procedural stage. Applicants need to know when an application is considered received, when verification begins, what constitutes completeness, and what happens if the system fails. These matters are technical in appearance but legal in effect because administrative deadlines and licensing status depend on them.

Digital licensing also has a transparency function. The ability to verify whether a professional has a valid practice licence can support supervision and reduce the risk of unlicensed practice. However, transparency does not mean that every piece of information stored in the licensing system should be publicly accessible. A legitimate distinction must be made between information necessary to verify professional authority and information that remains protected as personal data. Digital systems should therefore implement access according to the purpose and authority of each user.

The current framework is stronger than a purely paper-oriented licensing model in three identifiable respects: health law now provides an integrated information-system basis; implementing regulations structure electronic health-workforce administration and licensing timelines; and the Personal Data Protection Law adds enforceable data-processing principles and data-subject rights. The residual issue is not the absence of all rules but whether operational procedures sufficiently specify responsibility, correction, contingency, auditability, and restoration of a practitioner's legal position when interconnected systems produce an error.

Legal Protection of Anesthesia Practitioners' Personal Data

The data processed for digital licensing should be distinguished by legal function. General personal data may include name, national identity number, contact information, and address. Professional or administrative data include registration status, qualifications, education, employment history, practice location, and licensing records. Where the workflow also processes health data or biometric identifiers, those data may fall within the specific personal-data categories that receive heightened protection under Law Number 27 of 2022. The classification matters because lawful basis, access control, security, retention, and breach consequences must be proportionate to the sensitivity and purpose of the data.

Law Number 17 of 2023 contains specific provisions concerning health information systems. Article 351 requires health information system operators to protect the data and health information of individuals. It also provides that the

processing of health data involving individual information must be based on the consent of the data owner and/or another lawful basis for processing under personal data protection legislation. This provision is important because it places protection within the legal structure of health information management itself.⁸

The significance of Article 351 is that the obligation to protect data is directed to the operator of the health information system. In a digital licensing environment, the applicant has limited control over database security, access permissions, system architecture, and inter-institutional transfers after information is submitted. The operator therefore bears responsibilities proportionate to the level of control it exercises. This is consistent with the view that digital health platforms require clear allocation of responsibility for personal-data protection.

The Health Law also 1150epractises rights concerning the processing of health information. The data subject should be able to understand the purpose for which information is collected and should have meaningful access to mechanisms for reviewing and correcting information. This is especially relevant to professional licensing because inaccurate data may affect a person's legal authority to 1150practise. A right to correct data therefore has a direct connection with professional legal status and should not be treated merely as a privacy right.

Law Number 27 of 2022 complements sectoral health law by distinguishing general and specific personal data and by regulating lawful processing, data-subject rights, security, accountability, and personal-data breaches.⁹ For digital SIPPA, the lawful basis must be identified for each processing purpose rather than assumed merely from the existence of a platform. Processing required to perform statutory public functions may rest on legal authority, while additional or optional uses may require another recognized basis. Specific data, if processed, require security and governance measures commensurate with their sensitivity.

Purpose limitation is particularly important in an integrated health information environment. Information collected for licensing should not automatically be used for unrelated purposes without an appropriate legal basis. The broader the purposes attached to a dataset, the greater the potential for excessive processing or disclosure. A sound licensing system should therefore identify the purpose associated with each category of information and limit access and use to what is necessary for that purpose.

Data minimization is equally important. A licensing platform should process only information that is necessary and legally relevant to the licensing and health-workforce purposes for which the system is operated. The fact that a platform is technically capable of storing additional data does not provide a legal basis to collect them. Limiting the dataset also reduces the consequences of unauthorized access and simplifies responsibility for accuracy and retention.

Accuracy is another essential component of personal data protection. An error in a professional registration number or practice location can prevent the system from matching the applicant with an existing professional record. If the error is propagated across integrated databases, correcting it may become more

⁸Indonesia, Law Number 17 of 2023 on Health, State Gazette of the Republic of Indonesia Year 2023 Number 105, particularly art. 351.

⁹Indonesia, Law Number 27 of 2022 on Personal Data Protection, State Gazette of the Republic of Indonesia Year 2022 Number 196.

complicated. For that reason, applicants should be given an accessible mechanism to inspect relevant information and request correction. The system should also retain a trace of changes so that it can be determined when information was modified and by whom.

Security measures must protect personal data from unauthorized processing, unauthorized access, loss, alteration, or disclosure. In practical terms, this includes role-based access, authentication, activity logging, secure transmission and storage, backup and recovery arrangements, and an incident-response process. These measures are not merely desirable system features; they operationalize statutory duties of security and accountability owed by the party or parties that determine the purposes and means of processing and by processors acting on their instructions.

The official SATUSEHAT SDMK privacy policy identifies the Ministry of Health as the electronic-system operator, describes SATUSEHAT SDMK as an integrated health-workforce data platform, recognizes both general and specific personal data, and provides user mechanisms for access, updating, and correction.¹⁰ It also recognizes controller and processor concepts. These statements help map responsibility, but controller/processor status for a specific data flow remains function-specific: the party that determines the purpose and exercises control over a processing activity bears controller obligations for that activity, while a party processing on another controller's instructions acts as processor. A health facility, source-data institution, licensing authority, and the SATUSEHAT operator may therefore have different responsibilities for different stages of the same workflow.

Verification needs do not justify unrestricted disclosure. Information necessary to confirm professional authority may be made available to authorized users or through a public verification function, while identity, contact, employment-history, device, health, or biometric data should remain restricted unless disclosure has a lawful and proportionate basis. Purpose limitation, data minimization, and role-based access should therefore be reflected in the architecture of the licensing workflow.

From the perspective of legal protection, the position of the anesthesia practitioner can therefore be understood as involving two connected layers. The first layer arises from health law, which specifically requires protection of health information within the health information system. The second layer arises from the Personal Data Protection Law, which establishes broader rights and obligations concerning personal data. The two regimes should be read together because digital SIPPA operates at the intersection of professional administration and personal data processing.

The preventive dimension of legal protection is visible in the obligation to establish a secure and accountable system before any breach occurs. The repressive dimension becomes relevant when a breach, error, or unlawful processing has already occurred. Both are necessary. A system that has a complaint mechanism but weak preventive security is inadequate, while a highly secure system without a workable correction or complaint mechanism may still fail to protect a professional whose legal status has been affected by an administrative error.

¹⁰Ministry of Health of the Republic of Indonesia, "SATUSEHAT SDMK: Kebijakan Privasi," accessed September 8, 2026, <https://satusehat.kemkes.go.id/sdmk/privacy-policy>.

Legal Implications of System Disruptions, Data Errors, and Personal Data Breaches

The first projected risk category is service interruption. A digital channel may become unavailable or may fail to complete an upload, verification, or status update. This article does not assert that such events occur with a specified frequency. The legal analysis asks how a mandatory digital process should respond if an interruption occurs: the system should preserve incident logs and the applicant should be able to demonstrate attempted compliance through an alternative evidentiary route.

Minister of Health Regulation Number 13 of 2025 contains an important mechanism concerning the timing of SIP issuance. Under Article 154, a SIP is issued no later than five working days after the requirements are declared complete; if issuance exceeds that period, the SIP automatically becomes effective through the information system. The regulation also provides for electronic processing and related administrative mechanisms. This rule strengthens legal certainty because it reduces the possibility that an applicant will remain indefinitely dependent on an administrative process without a defined consequence for delay.¹¹

A second category is data mismatch. An application may be technically available but unable to progress because a professional record differs across connected systems. Responsibility should be allocated by source: applicant-supplied errors may require applicant correction; verified source-data errors should be corrected by the institution that controls the authoritative record; and integration or synchronization errors should be addressed by the operator responsible for the interface. The applicant should not be required to restart a complete licensing process where the underlying error is demonstrably administrative or systemic.

The right to correction is therefore both a data-protection right and an administrative legal-certainty mechanism. The practitioner should be able to identify the disputed field, submit supporting evidence, and direct the request to the institution that controls the relevant authoritative record or to the SATUSEHAT complaint/correction channel where the platform record is at issue. The available official policy permits users to update or correct certain self-submitted data and provides a written complaint channel.¹² Where a correction requires verification by another authority, the system should record the request, identify the responsible institution, and preserve the practitioner's proof of timely action. The positive-law materials reviewed do not establish a single uniform correction deadline for every cross-system data mismatch; this is a residual procedural gap that should be clarified by SOP or ministerial regulation.

A third category is a personal-data breach. The Personal Data Protection Law gives particular importance to sensitive categories such as health and biometric data, while the professional licensing environment may also expose identity and professional records. The legal consequence depends on what data were affected, which entity controlled the relevant processing purpose, the security measures

¹¹Indonesia, Minister of Health Regulation Number 13 of 2025 concerning the Management of Health Human Resources, arts. 154–156.

¹²Ministry of Health of the Republic of Indonesia, "SATUSEHAT SDMK: Kebijakan Privasi," accessed September 8, 2026, <https://satusehat.kemkes.go.id/sdmk/privacy-policy>.

required, and the statutory duties triggered by the incident.¹³ A breach should not be treated merely as an information-technology event where it also affects the practitioner's ability to demonstrate professional status or exposes data to misuse.

A data breach may also affect professional reputation and trust. Information about a health professional can reveal identity, professional qualifications, registration status, and practice location. If such information is combined with other leaked information, the consequences may include identity fraud, impersonation, or other forms of misuse. Even where no immediate financial loss is demonstrated, the loss of control over professional information can be a significant harm. The system operator should therefore treat incident response as both a technical and legal responsibility.

Digitalisation also changes the evidentiary dimension of licensing. This article addresses electronic logs primarily as administrative evidence of submission, verification, data alteration, and issuance, and secondarily as potential electronic evidence if a licensing dispute proceeds to administrative or judicial review. The value of logs depends on integrity, timestamps, access controls, and preservation. Audit trails should therefore allow the sequence of administrative actions to be reconstructed without treating an automated screen status as conclusive proof when contrary source records exist.

Preventive legal protection requires a defined contingency mechanism. At minimum, the system should: (1) record a verified technical incident; (2) provide an alternative submission or acknowledgement channel when the prescribed platform is unavailable; (3) preserve evidence of the applicant's attempted timely compliance; (4) suspend or extend a procedural deadline where non-compliance is caused by a verified system failure; and (5) permit a temporary manual or assisted process where necessary to prevent the practitioner from losing legal status solely because the electronic channel is inaccessible. These elements implement legal certainty and proportionality; they do not create a separate licence outside the competent authority's statutory power.

Repressive protection is required when an error has already caused harm. The practitioner should have access to correction, complaint, administrative review, and other remedies available under the applicable legal framework. Research on practice without SIP shows why the legal status of the licence matters: when licensing is a condition of lawful practice, an incorrect administrative record can have consequences for both professional activity and institutional responsibility.¹⁴

The principle of legal certainty is particularly relevant in these circumstances. Radbruch associates legal certainty with the function of law in providing an orderly and predictable framework, while Utrecht 1153 practises clear and non-contradictory rules. In digital licensing, certainty requires more than a formal regulation: the applicant must be able to predict how the system treats an application, how deadlines are calculated, and how errors are corrected.¹⁵

¹³Inggrit Rismauli Siahaan et al., "Analisis Praktik Perlindungan Data Pribadi pada Aplikasi 'SatuSehat' terhadap Regulasi Hukum di Indonesia," *Jurnal Teknoinfo* 18, no. 1 (2024): 141–150.

¹⁴A. Nurdin, U. Fitria, and K. A. Dinen, "Tanggung Jawab Hukum Praktik Tanpa Surat Izin Oleh Penata Anestesi di Rumah Sakit," *Public Health Journal* 1, no. 2 (2024).

¹⁵Gustav Radbruch, *Legal Philosophy* (Berkeley: University of California Press, 1973).

The implications of digitalization are therefore two-sided. On one side, electronic licensing can improve efficiency, transparency, and administrative control. On the other side, increased dependence on digital infrastructure creates a greater risk that a technical or data-related failure will affect legal rights. The appropriate response is not to reject digitalization, but to build legal safeguards into the system itself. The digital process should be designed around accountability rather than treating legal protection as a separate issue that arises only after a problem occurs.

Legal Protection and Legal Certainty for Anesthesia Practitioners

Legal protection in digital SIPPA must be evaluated against positive-law duties rather than abstract good-governance preferences. Preventive protection concerns clarity of authority, lawful and purpose-limited processing, accuracy, security, accessible correction, audit trails, and contingency. Repressive protection concerns incident response, restoration of inaccurate records, complaints or review, and accountability after a violation or administrative error.¹⁶

Preventive protection begins with clear information. An applicant should be able to identify the applicable requirements, understand which data are required, know which authority is responsible for the decision, and follow the progress of the application. Clear information reduces uncertainty and also reduces the possibility that an applicant will be considered non-compliant because of an unclear administrative instruction. Transparency is therefore not simply a service-quality issue; it is part of the legal protection afforded to the applicant.

Preventive protection also requires data governance. The system should collect only information that has a legitimate connection to the licensing purpose, restrict access according to user authority, maintain reliable records of changes, and implement appropriate security measures. These safeguards are especially important because the professional has limited control over the infrastructure after submitting the information. The more dependent the professional becomes on the system, the stronger the justification for placing clear accountability on the system operator.

When an application or data record is wrong, an effective correction route should specify four elements: the claimant and disputed field; the institution controlling the authoritative record; supporting evidence; and the legal or procedural effect of the pending correction. The official SATUSEHAT SDMK policy allows users to update or correct certain data and provides a complaint channel, but cross-institutional corrections may still depend on verification by the relevant source-data institution.¹⁷ For legal certainty, an SOP should set service standards and response times and should ensure that a pending correction caused by a verified administrative mismatch does not automatically prejudice the applicant's professional status.

The concept of legal certainty complements the analysis. Legal certainty requires norms that are clear, consistent, and capable of guiding conduct. Radbruch

¹⁶Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat di Indonesia* (Surabaya: PT Bina Ilmu, 1987).

¹⁷Ministry of Health of the Republic of Indonesia, "SATUSEHAT SDMK: Kebijakan Privasi," accessed September 8, 2026, <https://satusehat.kemkes.go.id/sdmk/privacy-policy>.

treats certainty as an essential function of law, while Utrecht connects certainty with clear rules that do not conflict with one another. For digital SIPPA, this means that the applicant should be able to identify the competent authority, applicable requirements, procedural deadlines, and available remedies.¹⁸

Compared with the earlier paper-oriented model, the current framework adds concrete normative layers: integrated health-information governance under the Health Law, more detailed health-workforce and electronic-licensing administration under Government Regulation Number 28 of 2024 and Minister of Health Regulation Number 13 of 2025, and a comprehensive personal-data regime under Law Number 27 of 2022. The improvement is therefore identifiable in data integration, procedural digitization, statutory data-subject rights, and regulated processing duties. The framework is not complete, however, where operational allocation of responsibility, cross-system correction, contingency, and remedy remain dependent on procedures that are not uniformly specified.

The main challenge lies in translating those norms into operational procedures. A regulation may recognise a right to correct data, but the right has limited practical value if the system does not provide a simple correction mechanism. Similarly, a legal obligation to protect personal data has limited effect if responsibility is unclear when several systems are connected. Legal certainty therefore depends on the implementation of the regulatory framework, including the design of administrative workflows and the allocation of institutional responsibility.¹⁹

Professional protection also requires coordination between the central government, local authorities, health facilities, and the institutions responsible for maintaining professional information. Each actor may hold a different part of the information required for licensing. If those records are inconsistent, the professional may become responsible in practice for resolving a problem that originated elsewhere. An accountable digital system should instead allow the relevant institutions to identify the source of an inconsistency and resolve it without shifting the burden unfairly to the applicant.

The same principle applies to personal data breaches. The professional is the data subject and should not be expected to bear the consequences of an incident solely because the data were submitted voluntarily for a lawful administrative purpose. Where the state requires the information for licensing, the processing must be accompanied by corresponding safeguards. The stronger the administrative necessity of submitting the data, the stronger the justification for requiring the system operator to maintain effective protection and a meaningful remedy.

The evaluation in Tables 1 and 2 shows that digital SIPPA already rests on a substantial normative foundation, but protection is uneven across operational indicators. Authority and lawful basis are comparatively clear at the level of statutes and regulations; security and data-subject rights have a legal basis but require role-specific implementation; cross-system correction, incident coordination, appeal/remedy routing, audit-trail access, and contingency require more detailed

¹⁸E. Utrecht, *Pengantar dalam Hukum Indonesia* (Jakarta: Ichtiar Baru Van Hoeve, 1958).

¹⁹Widagdo Rekso Negoro, "Perlindungan Hukum bagi Penata Anestesi di Fasilitas Kesehatan yang Tidak Terdapat Dokter Spesialis Anestesi," *PREPOTIF: Jurnal Kesehatan Masyarakat* 9, no. 1 (2025), <https://doi.org/10.31004/prepotif.v9i1.41355>.

operational rules. The central problem is therefore not whether digital licensing is legally permissible, but whether the administrative workflow can preserve a practitioner's legal position when the technology or data chain fails.

A legally sound digital licensing system should consequently be assessed not only by speed. It should enable an applicant to identify the competent authority, understand the processing purpose, submit data securely, correct an inaccurate record, preserve evidence of submission, obtain a decision within the applicable timeframe, and invoke a defined response when an incident occurs. Efficiency, data protection, and legal certainty must operate as one administrative design.

The overall relationship among the relevant regulations can be presented as follows.

Table 1. Allocation of Legal Obligations and Practitioner Protection in Digital SIPPA

Legal instrument	Core obligation	Responsible actor	Practitioner right/interest
Law Number 17 of 2023 on Health	Integrated health-information governance; protection of individual health information	Health-information system operator and competent public authority	Lawful, accurate and protected administration of professional information
Law Number 27 of 2022 on Personal Data Protection	Lawful basis, purpose limitation, accuracy, security, data-subject rights, breach response	Controller(s) and processor(s) according to the specific processing function	Access, correction, security, accountability and remedies for unlawful processing
Government Regulation Number 28 of 2024	Operational health-sector licensing and information-system implementation	Competent health/licensing authorities	Traceable and procedurally lawful licensing process
Minister of Health Regulation Number 13 of 2025	Health-human-resources management and electronic licensing administration	Competent licensing and health-workforce authorities	Defined licensing procedure and timing, including consequences of administrative delay
Minister of Health Decree HK.01.07/Menkes/722/2020	Professional standards for Penata Anestesi	Profession, facilities and relevant authorities	Recognition of professional competence and scope

Table 1 maps the principal regulatory instruments to obligations and responsible actors, while Table 2 evaluates the operational safeguards needed to translate those rules into effective legal protection. The matrices distinguish existing legal duties from recommended SOP or regulatory refinements, thereby avoiding the assumption that every projected digital risk already represents a documented system failure.

Table 2. Evaluation Matrix for Legal Protection in Digital SIPPA

Evaluation indicator	Current normative basis	Assessment	Operational response
Authority	Health Law and licensing regulations	Substantially clear at normative level	Display competent decision-maker and attribution of every status/decision
Lawful basis and purpose	Health Law; PDP Law; SATUSEHAT privacy governance	Legal basis exists; purpose mapping must be function-specific	Document purpose and legal basis for each data flow
Security	PDP Law; Health Law	Legal duty exists; implementation is system-specific	Role-based access, authentication, logging, secure transfer, backup and incident plan
Correction	PDP rights; SATUSEHAT user correction/complaint features	Partly specified; cross-system routing may be unclear	Source-record routing, service standard, proof of pending correction
Incident response	PDP Law and sectoral duties	Normative basis exists; coordination must be allocated	Define controller/processor roles and incident escalation
Appeal/remedy	Administrative and data-protection remedies	Potentially fragmented across institutions	Single visible complaint route with referral to competent body
Audit trail	Electronic administration and accountability principles	Technically feasible; access/preservation standards need detail	Immutable timestamps, change history and evidentiary preservation
Contingency	Legal certainty and proportional administration	Residual procedural gap	Verified outage record, fallback submission, deadline protection, temporary assisted/manual process

The anesthesia practitioner should remain visible throughout the process as a data subject and as the holder of professional rights. The professional is not merely a user entering information into an application. Personal and professional information is processed as part of an administrative decision, so a data-processing

error may simultaneously become a privacy issue and a licensing issue. The protection of both interests should therefore be integrated rather than treated as separate administrative concerns.

Digitalization should simplify administration without reducing professional rights. The priority reforms can be sequenced by legal level. At the SOP and system-feature level, authorities can improve acknowledgement receipts, audit trails, correction routing, incident logs, and fallback channels. At ministerial-regulation level, service standards can clarify cross-system correction, verified system failure, deadline effects, and responsibility among connected institutions. Higher-level legislative amendment should be reserved for gaps that cannot be resolved within existing statutory authority, rather than treating every operational problem as a reason to enact a new law.

CONCLUSION

First, digital SIPPA is governed by an interconnected framework of health-professional licensing, digital administration, and personal-data protection. Law Number 17 of 2023, Government Regulation Number 28 of 2024, and Minister of Health Regulation Number 13 of 2025 provide the licensing and health-information structure, while Law Number 27 of 2022 governs personal-data processing. SATUSEHAT SDMP is an integrated data and service platform; the legality of a licence remains attributable to the competent administrative authority rather than to the interface itself.

Second, anesthesia practitioners hold a dual legal position as licensing applicants and data subjects. Their general identity and professional data must be processed for a defined licensing purpose, while any specific personal data require safeguards appropriate to their sensitivity. The framework recognizes security, accuracy, access, correction, and incident-response duties, but responsibility must be mapped by processing function among the platform operator, licensing authority, health facilities, and source-data institutions.

Third, the principal residual risks concern cross-system correction, evidence of timely compliance, auditability, incident coordination, and contingency when a mandatory digital channel fails. These are projected legal risks unless supported by a documented incident. The priority response is therefore operational: detailed SOPs, reliable acknowledgement and audit trails, role-specific correction routing, incident procedures, and a fallback mechanism that prevents verified system failure from automatically prejudicing professional status. Ministerial rules may be required where uniform service standards or deadline effects cannot be secured by SOP alone.

This study is limited to normative materials and official policy documents. It does not include interviews, observation of licensing offices, practitioner surveys, or system-incident data and therefore cannot assess implementation effectiveness, user experience, or the frequency of digital failures. Future empirical research should test the evaluation indicators developed here against actual practitioner and licensing-authority experience.

REFERENCES

- Hadjon, Philipus M. *Perlindungan Hukum bagi Rakyat di Indonesia*. Surabaya: PT Bina Ilmu, 1987.
- Indonesia. *Government Regulation Number 28 of 2024 concerning the Implementing Regulation of Law Number 17 of 2023 on Health*. State Gazette of the Republic of Indonesia Year 2024 Number 135.
- . *Law Number 17 of 2023 on Health*. State Gazette of the Republic of Indonesia Year 2023 Number 105.
- . *Law Number 27 of 2022 on Personal Data Protection*. State Gazette of the Republic of Indonesia Year 2022 Number 196.
- . *Minister of Health Regulation Number 13 of 2025 concerning the Management of Health Human Resources*.
- Kumala, Rina, Hendra Suherman, dan Deaf Wahyuni. "Efektivitas Regulasi Penyelenggaraan Praktik Penata Anestesi dengan STRPA dan SIPPA dalam Pelayanan Anestesiologi Perioperatif." *Jurnal Kebijakan Kesehatan Indonesia* 12, no. 1 (2023): 22–26. <https://doi.org/10.22146/jkki.81459>.
- Manela, C., R. Sawitri, dan E. Prawestiningtyas. "Analysis of Medical Responsibility in the Era of Electronic Medical Records in Indonesia." *Soepa J. Health Law* 10, no. 2 (2024): 301–310. <https://doi.org/10.24167/Shk.V10i2.11411>.
- Ministry of Health of the Republic of Indonesia. "SATUSEHAT SDM: Kebijakan Privasi." Diakses pada 8 September 2026. <https://satusehat.kemkes.go.id/sdmk/privacy-policy>.
- Nasution, Erdi Effendi, Marice Simarmata, dan Muhammad Arif Sahlepi. "Legal Analysis of Hospital Responsibilities in Implementing Electronic Medical Records Integrated with Satu Sehat." *Proceedings of International Conference on Islamic Community Studies*, 2025.
- Negoro, Widagdo Rekso. "Perlindungan Hukum bagi Penata Anestesi di Fasilitas Kesehatan yang Tidak Terdapat Dokter Spesialis Anestesi." *PREPOTIF: Jurnal Kesehatan Masyarakat* 9, no. 1 (2025). <https://doi.org/10.31004/prepotif.v9i1.41355>.
- Nurdin, A., U. Fitria, dan K. A. Dinen. "Tanggung Jawab Hukum Praktik Tanpa Surat Izin Oleh Penata Anestesi di Rumah Sakit." *Public Health Journal* 1, no. 2 (2024).
- Purwaningsih, Aditya Dwi, dan Purnawan Junadi. "Kebijakan Penerbitan Surat Tanda Registrasi Bagi Tenaga Medis dan Tenaga Kesehatan: Literature Review." *Jurnal Ners* 9, no. 4 (2025): 7898–7904. <https://doi.org/10.31004/jn.v9i4.51130>.
- Radbruch, Gustav. *Legal Philosophy*. Berkeley: University of California Press, 1973.
- Rahardjo, Satjipto. *Ilmu Hukum*. Bandung: Citra Aditya Bakti, 2000.
- Rusmana, R., dan I. Sari. "Analysis of the Implementation of the Generic Regional Health Information System (Sikda) to Support the Effectiveness of Electronic

- Medical Records at the Campaka Community Health Center Uptd." *J. Med. Record and Health Information* 4, no. 4 (2023): 203–212. <https://doi.org/10.25047/J-Remi.V4i4.3956>.
- Siahaan, Inggrit Rismauli, et al. "Analisis Praktik Perlindungan Data Pribadi pada Aplikasi 'SatuSehat' terhadap Regulasi Hukum di Indonesia." *Jurnal Teknoinfo* 18, no. 1 (2024): 141–150.
- Tektona, Rahmadi Indra, Fendi Setyawan, dan Frederica Prima. "Kepastian Hukum Pemilik Data Pribadi Dalam Aplikasi Satu Sehat." *Jurnal Legislasi Indonesia* 20, no. 1 (2023): 28–41. <https://doi.org/10.54629/jli.v20i1.996>.
- Utrecht, E. *Pengantar dalam Hukum Indonesia*. Jakarta: Ichtiar Baru Van Hoeve, 1958.
- Wahyudi, A., D. Nurhidayati, dan R. Setiawan. "Implementasi KMK Nomor HK.01.07/MENKES/722/2020 tentang Standar Profesi Penata Anestesi di Indonesia." *Jurnal Kebijakan Kesehatan Indonesia* (2023).
- Wahyudiono, Gunawan, Joko Ismono, dan Nuryanto A. Daim. "Perlindungan Hukum Tenaga Kesehatan (Penata Anestesi) Setelah Terbitnya Undang-Undang Kesehatan Nomor 17 Tahun 2023." *Law and Humanity* 2, no. 1 (2024): 1–17. <https://doi.org/10.37504/lh.v2i1.605>.