

## Strategi Perlindungan Data Diri Pasien Sebagai Bentuk Aplikasi Prinsip Etik Keperawatan *Confidentiality*: Kajian Literatur

Nur Cita Qomariyah<sup>1</sup> Wiwik Kusumawati<sup>2</sup>

<sup>1,2</sup> Magister Keperawatan Universitas Muhammadiyah Yogyakarta, Indonesia

Email: <sup>1</sup>nurcitaumy2025@gmail.com

<sup>2</sup>wiwik@umy.ac.id

### Abstrak

Perkembangan teknologi informasi dan digitalisasi rekam medis membawa sebuah ancaman digital pada perlindungan data diri pasien. Hal ini akan menyebabkan munculnya resiko penyalahgunaan data dan akses yang tidak sah pada data diri pasien. Penelitian ini bertujuan untuk menelusuri lebih lanjut terkait strategi dan langkah-langkah efektif yang dapat dilakukan dalam upaya menjaga kerahasiaan data diri pasien di sebuah pelayanan kesehatan. Penelitian ini menggunakan metode studi literatur sistematis dengan PRISMA. Pencarian data dilakukan melalui *database* Scopus dengan kriteria artikel yang digunakan adalah artikel yang terbit tahun 2021-2025 dan menggunakan Bahasa Inggris. Hasil pencarian didapatkan 6 artikel yang relevan dan dilakukan analisis yang lebih dalam. Hasil telaah menunjukkan empat strategi utama dalam menjaga kerahasiaan data pasien: Perlindungan teknis data pasien, peningkatan literasi, audit dan evaluasi sistem, dan kampanye serta sosialisasi. Penerapan empat strategi ini dapat mengurangi kemungkinan pelanggaran dan penyalahgunaan data diri pasien, meningkatkan etika profesional keperawatan dan meningkatkan kepercayaan masyarakat terhadap layanan kesehatan

**Kata kunci:** *Confidentiality*, Keperawatan, Perlindungan Data Diri, Privasi Digital, Strategi Keamanan

### Abstract

*The development of information technology and the digitalization of medical records have introduced new digital threats to the protection of patients' personal data. These developments increase the risk of data misuse and unauthorized access to patient information. This study aims to further explore effective strategies and measures that can be implemented to safeguard patient data confidentiality within healthcare services. A systematic literature review was conducted using the PRISMA approach. Data were retrieved from the Scopus database with inclusion criteria comprising English-language articles published between 2021 and 2025. The search identified six relevant articles, which were subsequently analyzed in depth. The review findings highlight four primary strategies for maintaining patient data confidentiality: technical protection of patient data, literacy enhancement, system audits and evaluations, as well as campaigns and public outreach. The implementation of these four strategies can reduce the likelihood of data breaches and misuse, strengthen nursing professional ethics, and enhance public trust in healthcare services.*

**Keywords:** *Confidentiality, Digital Privacy, Nursing, Personal Data Protection, Security Strategies*

## 1. PENDAHULUAN

Praktik perlindungan data diri pasien saat memberikan pelayanan kerap kali menghadapi berbagai tantangan terutama dengan adanya perkembangan teknologi dan informasi serta digitalisasi rekam medis. Selain karena semakin majunya teknologi, kurangnya pengetahuan tenaga kesehatan terhadap menjaga rahasia pasien itu juga memicu terjadinya pelanggaran baik secara sengaja atau tidak di sengaja (Widjaja, et al, 2025). Kejadian penyalahgunaan data pribadi pasien pernah terjadi di Indonesia tahun 2020 pada saat Covid 19 melanda. Sebanyak 230 ribu data tes Covid 19 warga Indonesia pada saat itu ditampilkan secara online, dimana data tersebut mencakup dari data pribadi sampai ke hasil pemeriksaan Covid 19. Regulasi terkait perlindungan data pribadi sudah diatur dalam Undang-Undang Republik Indonesia Nomor 27 Tahun 2022. Undang-Undang

dasar Negara Republik Indonesia juga mengatur terkait perlindungan privasi dan data penduduk dalam pasal 28 G ayat 1 yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari sebuah ancaman. Penyebaran data pribadi diatas tentunya selain menyalahi regulasi yang sudah ada dan juga menyalahi kode etik keperawatan yaitu *confidentiality* dimana perawat harus mampu menjaga kerahasiaan data diri pasien.

Prinsip etik *confidentiality* menekankan bahwa perawat harus menjaga kerahasiaan pasien. Kewajiban menjaga rahasia medis diatur di dalam Permenkes Nomor 36 tahun 2012, dimana pasal 3 menyebutkan rahasia kedokteran mencakup data dan informasi mengenai identitas pasien, kesehatan pasien meliputi hasil anamnesis, pemeriksaan fisik, pemeriksaan penunjang, penegakan diagnosis, pengobatan, tindakan kedokteran dan hal lain yang berkenaan dengan pasien (Permenkes, 2012). Prinsip kerahasiaan ini menjelaskan bahwa segala informasi yang diketahui oleh perawat mengenai permasalahan yang dialami oleh klien, perawat tidak berhak untuk menyebarluaskan informasi meskipun klien tersebut meninggal, terkecuali apabila perawat telah mendapatkan persetujuan dari klien dengan menyertakan surat persetujuan (Munandar, et al., 2022). Meskipun sudah ada regulasi dan kode etik yang ada, faktor kemajuan teknologi juga dapat meningkatkan resiko terjadinya penyalahgunaan dan penyebaran data diri pasien.

Semakin maju dan berkembangnya teknologi yang ada membuat ancaman penyebaran data diri pasien secara digital semakin meningkat. Beberapa kejadian kebocoran data yang terjadi menunjukkan bahwa sistem keamanan data digital yang ada di Indonesia masih terbilang lemah. Hal ini menimbulkan menurunnya tingkat kepercayaan masyarakat, padahal kepercayaan sangat penting terbentuk antara pemberi pelayanan dengan seorang pasien (Indiastari et al., 2023). Salah satu dasar kepercayaan ini adalah keyakinan bahwa tenaga kesehatan tidak akan membagikan informasi medis apa pun kepada pasien karena setiap pasien berhak atas rahasia medis, dimana hal tersebut merupakan etika profesi yang harus dilindungi oleh hukum dan peraturan masyarakat (Widjaja, Sijabat, et al., 2025).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 mengatur bahwa perlindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. Data pribadi termasuk data umum dan data spesifik. Data spesifik seperti data informasi kesehatan, genetika, catatan kejahatan dan lain-lain. Kode etik dari setiap profesi kesehatan juga sudah mengatur terkait kewajiban menjaga data diri pasien yakni prinsip etik *confidentiality*. Regulasi yang sudah ada tidak tersosialisasikan dengan baik, sehingga masyarakat di Indonesia belum memahami pentingnya perlindungan data diri. Penyebab lainnya yang membuat pelanggaran ini terjadi adalah rendahnya literasi digital sehingga mereka sangat berpotensi mengalami berbagai bentuk penyalahgunaan data pribadi seperti penipuan dan lain sebagainya (Natamiharja, et al., 2024).

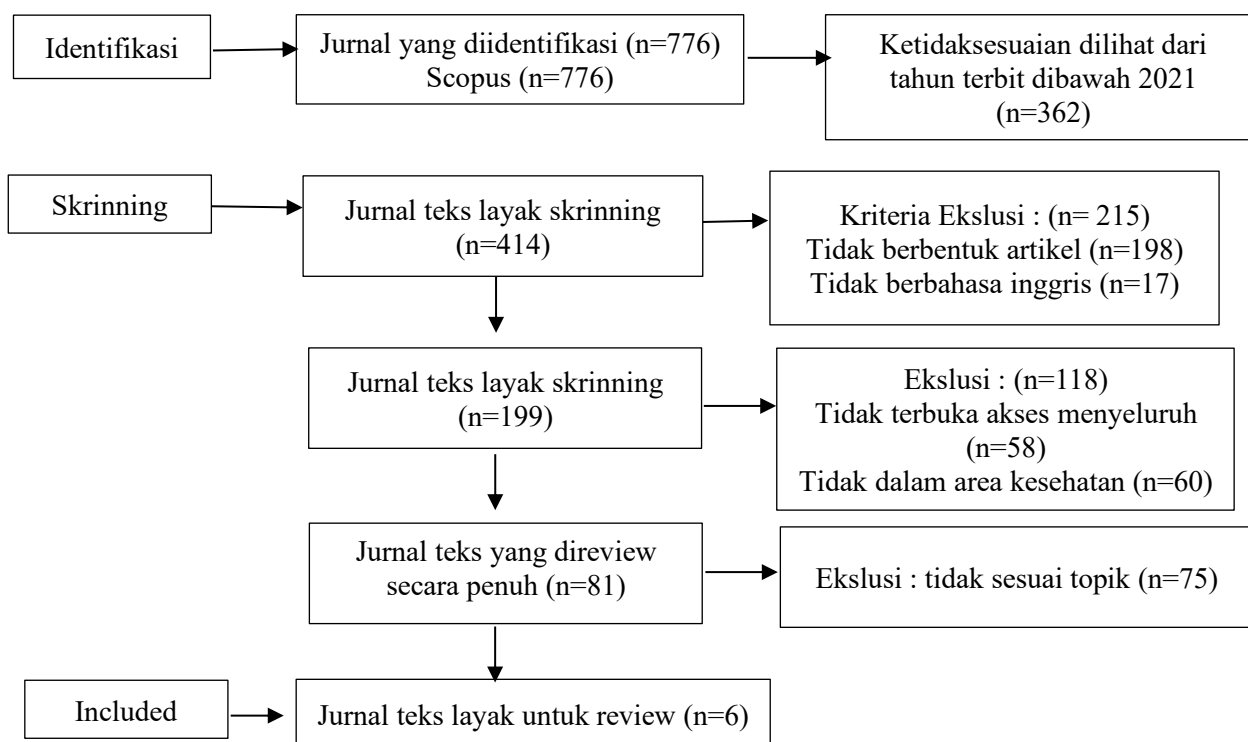
Beberapa contoh kasus penyebaran data diri pasien yang dilakukan oleh tenaga kesehatan yakni seorang perawat yang bekerja sebagai petugas asuransi melakukan *doxing* data pribadi pasien ke status media sosialnya yaitu whatsapp. Hal yang dilakukan perawat ini melanggar Peraturan Menteri Kesehatan Nomor 36 Tahun 2012 tentang Rahasia Kedokteran dimana mewajibkan semua pihak yang terlibat dalam pelayanan wajib menyimpan rahasia kedokteran. Tak berselang lama, kejadian ini langsung viral dan membuat pasien marah dan melakukan tuntutan dari tindakan yang dilakukan oleh perawat tersebut (Pos Kota, 2025). Perawat berakhir di pecat dari pekerjaannya dan juga harus menghadapi tuntutan hukum yang dilyangkan oleh pasien. Seorang nakes juga pernah melakukan *live streaming* tiktok saat pasien proses melahirkan dan berujung nakes tersebut dikenakan sanksi etik oleh organisasi profesi terkait.

Konsekuensi hukum dari pelanggaran tenaga kesehatan terhadap tanggung jawab menjaga rahasia medis tidak boleh dianggap remeh. Jika seseorang melakukan pelanggaran apa pun, mereka dapat menghadapi sanksi administratif, sanksi etik, atau bahkan sanksi pidana, seperti yang diatur dalam Pasal 322 Kitab Undang-Undang Hukum Pidana (KUHP). Hal ini menunjukkan bahwa menjaga rahasia medis adalah tugas yang penting dan harus dilakukan dengan benar (Handayani, 2024). Pelanggaran rahasia medis dapat membahayakan reputasi tenaga kesehatan dan institusi

pelayanan kesehatan selain perihal alasan hukum. Apabila terjadi kebocoran data medis yang melibatkan tenaga kesehatan, kepercayaan masyarakat terhadap layanan kesehatan dapat menurun (Widjaja et al., 2025). Sistem digitalisasi rekam medis yang dilakukan saat ini membuat perlindungan data diri pasien lebih rawan mengalami penyalahgunaan dan penyebaran data pasien. Belum banyak penelitian yang mengintegrasikan aspek hukum, etika dan strategi yang dapat dilakukan guna mengoptimalkan perlindungan data diri pasien. Penelitian ini bertujuan untuk menganalisis strategi efektif penerapan prinsip confidentiality dalam menjaga data pribadi pasien berdasarkan telaah literatur nasional dan internasional.

## 2. METODE PENELITIAN

Kajian pada penulisan ini menggunakan metode studi literatur sistematis. Studi literatur adalah jenis penelitian yang dilakukan melalui melihat kembali berbagai kajian kepustakaan yang dibutuhkan untuk penelitian. Pendekatan ini bertujuan untuk menganalisis penelitian terdahulu sebagai sumber yang relevan dengan topik perlindungan data diri pasien. Secara teori, studi literatur merupakan sebuah proses pencarian sumber sesuai dengan topik yang diinginkan, setelah itu data di proses dan akan didapatkan hasil (Febrianto et al., 2024). Sumber data yang digunakan di penelitian ini yaitu sumber data primer dan sekunder. Sumber data primer meliputi data hasil penelitian, laporan penelitian, jurnal ilmiah, dan sebagainya, sementara sumber data sekunder yakni peraturan berdasarkan hukum, pemerintah, buku dan lain-lain (Nurjannah & Mukarromah, 2021). Artikel yang digunakan dalam studi literatur ini adalah artikel yang didapatkan dengan menggunakan database yaitu *Scopus* dari tahun 2021-2025 dengan memasukkan kata kunci dalam Bahasa Inggris dengan kata kunci “*Strategy for Protection*” OR “*Implementation of Personal Data Protection*”, AND “*Patient’s Personal Data*”, AND “*Confidentiality*” dengan total jumlah 6 artikel yang memenuhi syarat dan dilakukan analisis terlebih lanjut. Penulisan dan penyusunan daftar Pustaka pada penelitian ini menggunakan aplikasi *Mendeley*.



### 3. HASIL DAN PEMBAHASAN

Tabel 1 Ringkasan Jurnal

No	Penulis	Tahun Terbit	Judul Jurnal	Tujuan Penelitian	Hasil Penelitian
1	Chen, et al,	2025	<i>Protecting Radiology Data and Devices Against Cybersecurity Threats : A Joint White Paper of the ACR and Society for Imaging Informatics in Medicine</i>	Mengkaji strategi untuk meningkatkan sistem pencitraan medis, memberikan pelatihan kepada tenaga Kesehatan dan membangun pendekatan respon insiden untuk serangan siber dan pelanggaran data	Langkah - Langkah yang bisa dilakukan : 1. Mengontrol akses 2. Mengamankan perangkat sistem 3. Melakukan inventarisasi sistem yang rentan dan pembaruan patch keamanan secara teratur 4. Pemantauan dan audit sistem secara berkala
2	Alanazi	2025	<i>Assessing Clinicians' Legal Concerns and the Need for a Regulatory Framework for AI in Healthcare : A Mixed-Methods Study</i>	Penelitian ini bertujuan untuk memberikan rekomendasi terkait kerangka hukum awal dalam pengembangan integrasi teknologi AI ke sistem kesehatan	Langkah-Langkah yang bisa dilakukan : 1. Menciptakan UU perlindungan data pribadi 2. Meningkatkan literasi terkait perlindungan data diri pasien 3. Membangun sistem pelaporan Insiden
3	Semyonov	2024	<i>Keeping Medical Information Safe and Confidential : a qualitative study on Perceptions of Israeli Physicians</i>	Untuk memahami pandangan dan praktik dokter rumah sakit dalam menjaga informasi medis pasien	Langkah konkret yang bisa dilakukan : 1. Memantau kepatuhan terkait kebijakan yang ada 2. Memberikan konsekuensi bagi pelanggaran yang dilakukan
4	Subramanian & Xu	2024	<i>Patient Health Record Protection Beyond the Health Insurance Portability and Accountability Act : Mixed Methods Study</i>	Untuk menganalisis data pelanggaran perawatan Kesehatan di rumah sakit dan membandingkannya dengan tingkat kepatuhan HIPAA (Health Insurance Portability and Accountability Act)	Strategi perlindungan data pasien : 1. Pelatihan Karyawan 2. Penetapan prosedur kebijakan 3. Kontrol akses, enkripsi dan alat audit
5	Mocydlarz, et al	2023	<i>Management of Onsite and remote Communication</i>	Untuk mengevaluasi isu-isu yang muncul terkait sistem perlindungan data	Langkah-Langkah yang dilakukan : 1. Melakukan proses otentikasi yang kuat

		<i>in Oncology Hospitals : data Protection in an Era of Rapid Technological Advances</i>	dan keamanan pelayanan Kesehatan di rumah sakit onkologi	2. Adanya kontrol data secara berkala 3. Memperbarui sistem yang ada dengan teknologi baru
6	Schmitt, Tugce	2023 <i>Implementing Electronic Health Record in Germay : Lessons (Yet to Be) Learned</i>	Untuk menganalisis faktor-faktor yang mempengaruhi implementasi <i>electronic health record</i>	Langkah-Langkah yang bisa dilakukan : 1. Peningkatan kontrol data pasien 2. Peningkatan literasi 3. Kampanye informasi dan penggunaan aplikasi yang mudah diakses

Perlindungan atas kerahasiaan dan privasi pasien tentang data diri dan informasi penyakitnya saat menjalani asuhan keperawatan termasuk dalam hak-hak pasien yang harus terpenuhi. Membuka data dan melakukan penyebaran data tanpa izin tidak dibenarkan karena bersifat melanggar hukum dan menimbulkan kerugian pada pasien baik material maupun immaterial (Saputra, 2023). Peraturan perlindungan data pribadi pada sektor Kesehatan diatur di Undang-Undang No 27 Tahun 2022, dimana diatur bahwa data pribadi dibagi menjadi dua yaitu data pribadi spesifik dan data pribadi umum. Kedua data pribadi ini wajib di lindungi berdasarkan undang-undang yang berlaku. Pemberian sanksi bagi pelanggaran penyalahgunaan data sudah diberikan mulai baik dari segi perdata maupun pidana, namun penyebebaran data masih terus terjadi. Hal ini kemungkinan disebabkan belum adanya analisis terkait kepatuhan terhadap peraturan yang sudah ada seperti yang sudah diterapkan di Eropa yaitu *General Data Protection regulation* (GDPR) (Widjaja, et al., 2025).

GDPR yang diterapkan di Eropa menggunakan pendekatan yang berbasis hak asasi manusia dimana semua orang memiliki kesempatan yang sama dalam mendapatkan perlindungan data diri. Prinsip dasar yang diterapkan oleh GDPR adalah integritas, kerahasiaan data, legalitas, transparan, akurasi dan minimisasi data. Penelitian yang dilakukan oleh Kaendo & Ade, (2025) membandingkan tentang regulasi perlindungan data diri di Indonesia dan Eropa. Hasil penelitian menunjukkan adanya perbedaan dalam cara pasien mengakses data pribadi dan institusi pengawas. Sistem GDPR individu mampu melakukan pengajuan penghapusan data pribadi secara langsung melalui pengendali data secara cepat tanpa harus melalui proses pengadilan, sementara pada Indonesia pengajuan penghapusan data harus melewati keputusan pengadilan. Lembaga pengawasan yang ada di Indonesia sudah disahkan dalam UU PDP, namun lembaga tersebut belum optimal dalam melakukan tugas-tugasnya sehingga masih terjadi pelanggaran terjadi. Pelanggaran penyebaran data yang dilakukan oleh perawat ini juga mencederai kode etik keperawatan.

Perawat dalam melakukan pemberian asuhan keperawatan sehari-hari harus menerapkan dan menjunjung tinggi prinsip etik keperawatan salah satunya yaitu prinsip etik *confidentiality*. *Confidentiality* adalah sebuah prinsip yang menjaga kerahasiaan pasien baik identitas, kondisi atau bahkan perkembangan kondisi pasien. Perawat harus mampu menjaga kerahasiaan informasi pasien baik data pribadi spesifik atau umum sesuai dengan prinsip etik dan peraturan yang berlaku. Kebijakan perlindungan data diri pasien ini juga sesuai dengan teori *bioethic* dari Beauchamp & Childress (2019) dimana perlindungan data diri adalah sebagai bentuk menghargai otonomi pasien dan mencegah terjadinya kerugian yang berlanjut pada pasien (*non-maleficience*). Namun pada kenyataannya, praktik perlindungan data pribadi pasien ini sering mengalami hambatan dalam pelaksanaannya.

Hambatan yang sering muncul adalah adanya kurangnya infrastruktur yang memadai, kurangnya pengetahuan terkait pentingnya menjaga kerahasiaan data dan adanya serangan

peretasan eksternal (Pradana & Wilma, 2024 ; Lubis et all, 2024 ; Budiman, et all, 2025). Sebagian rumah sakit di daerah mengalami keterbatasan infrastruktur sarana dan prasarana, bahkan beberapa rumah sakit belum memiliki keamana siber seperti antivirus. Rendahnya pemahaman dari tenaga kesehatan dan non kesehatan yang bekerja di rumah sakit terkait peraturan perlindungan data pribadi pasien juga menjadi hambatan dalam pelaksanaan di lapangan (Pradana dan Wilma, 2024). Menjaga data pribadi pasien adalah sebuah hal yang mutlak dilakukan oleh pelayanan kesehatan. Perlindungan data yang kuat tidak hanya mematuhi peraturan yang ada namun juga mencegah agar tidak terjadi penyalahgunaan data pribadi pasien dan menjaga mutu pelayanan yang berintegritas. Berdasarkan hasil dari *literature review* terhadap 6 artikel terkait, terdapat berbagai strategi yang efektif dapat dilakukan untuk melindungi data pribadi pasien sebagai bentuk penerapan prinsip etik *confidentiality*. yaitu:

### **Perlindungan Teknis Data Pasien**

Perlindungan data diri pasien melalui sebuah sistem yang terintegrasi penting untuk dilakukan. Rumah sakit dan lembaga kesehatan lainnya harus memperbaiki infrastruktur dan sistem teknologi yang digunakan untuk rekam medis elektronik. Pembangunan infrastruktur teknologi informasi adalah langkah pertama menuju strategi pengendalian data mendasar dan menyeluruh. Penelitian yang dilakukan oleh Ardianto & Nurjanah (2024) menunjukkan bahwa penyalahgunaan data rekam medis pasien salah satunya disebabkan oleh kurangnya fitur penggantian password data secara berkala. Penelitian lain yang dilakukan oleh Sofia et all., (2022) menunjukkan bahwa aspek penting dalam menjaga kerahasiaan data pasien adalah autentikasi (tanda tangan elektronik) dan kontrol akses. Perlindungan data pasien dapat dilakukan dengan enkripsi data, sistem autentikasi ganda, dan penggunaan server yang aman (Pradana dan Wilma, 2024). Enkripsi adalah sebuah proses dimana mengubah data menjadi sebuah bentuk sebuah kode yang tidak dapat dibaca secara langsung dan hanya dipahami oleh individu yang berwenang saja sehingga meminimalisir terjadinya penyalahgunaan data (Alisa A & Yogi P, 2024).

Data pasien yang disimpan di sistem rumah sakit harus dienkripsi, baik saat disimpan maupun saat dikirimkan. Orang yang tidak berwenang tidak dapat mengakses data yang dienkripsi dan dapat melindungi data pribadi dari akses yang tidak sah (Candra, et all, 2025). Selain enkripsi, otentikasi juga harus dilakukan dimana petugas akan diminta memasukkan identitasnya seperti kode sandi atau kode verifikasi yang dikirimkan ke akun yang terdaftar (Candra, et all, 2025). Penelitian yang dilakukan oleh Lestari & Rohman (2025) menunjukkan pada aspek autentikasi, setiap tenaga kesehatan terkait memiliki akun pribadi masing-masing. Wewenang untuk melakukan edit atau mengubah konten tidak dapat dilakukan oleh semua karyawan dan hanya bisa dilakukan oleh karyawan tertentu saja. Perubahan data yang dilakukan tidak mengubah data sebelumnya, namun hanya memberikan penanda sebuah garis merah pada data sebelumnya sebagai petunjuk bahwa data ini telah dilakukan modifikasi. Perlindungan data diri ini dapat diterapkan jika masing-masing rumah sakit memiliki infrastruktur dan teknologi yang memadai. Perbaikan dan peningkatan keamanan data pasien di Indonesia harus lebih diperkuat kembali karena pelanggaran penyebaran data pribadi masih terus terjadi.

### **Peningkatan Literasi**

Hal yang sangat penting untuk dilakukan yaitu meningkatkan kesadaran dan pengetahuan baik tenaga kesehatan maupun non kesehatan di rumah sakit tentang pentingnya menjaga kerahasiaan klien. Belum meratanya terkait pengetahuan perlindungan privasi klien inilah yang menyebabkan sering kali terjadi adanya pengaksesan data tanpa izin dan penyebaran data pribadi klien (*doxing*) (Pradana & Wilma, 2024). Adanya persepsi bahwa yang bertugas menjaga kerahasiaan data pasien hanya tim Teknologi Informasi (TI) saja juga menjadi salah satu sebab mminimnya literasi digital. Pelatihan terkait kemananan siber harus diberikan kepada seluruh tenaga kesehatan dan non kesehatan yang berkaitan dalam proses pemberian asuhan. Pembuatan SOP yang mengatur perlindungan data diri pasien juga harus dilakukan dimana didalamnya mencakup terkait klasifikasi

kerahasiaan, cara mengakses sistem hingga sanksi dari pelanggaran yang terjadi (Shakila & Ayu, 2025). Hal penting yang perlu ditanamkan pada semua tenaga kesehatan dan non kesehatan yang terlibat adalah dalam bekerja ada kode etik yang harus dijunjung tinggi dan ketika melanggar kode etik akan mendapatkan sanksi (Jiang, 2023). Pelatihan yang berulang terkait pentingnya menjaga data pribadi pasien sebaiknya masuk kedalam program kerja bulanan yang harus dilakukan setiap ruangan dengan harapan dapat membuat tenaga kesehatan dan non kesehatan yang bekerja selalu menjaga data pribadi pasien dan tidak melakukan pelanggaran.

### **Audit dan Evaluasi Sistem**

Sistem manajemen data pasien harus selalu diperbarui agar tetap aman dari kerentanan dan ancaman eksternal. Pembaruan perangkat lunak dan patch keamanan harus dilakukan sesegera mungkin begitu tersedia untuk menutup celah yang bisa dimanfaatkan oleh penyerang (Pradana & Wilma, 2024). Audit keamanan data harus dilakukan secara berkesinambungan guna mendeteksi dan menanggulangi adanya kesalahan dan kelemahan sistem. Audit yang dilakukan meliputi pengujian penetrasi, evaluasi kebijakan yang sudah ada, serta simulasi respon cepat tanggap saat terjadi kebocoran data (Kasad, 2023). Pelaksanaan praktik audit ini pada kenyataannya masih mengalami hambatan dikarenakan berbagai institusi masih menggunakan aplikasi yang gratis dan memiliki perlindungan yang tidak maksimal sehingga audit dan evaluasi yang dilakukan juga tidak bisa dilakukan secara optimal. Mahalnya biaya perawatan sistem aplikasi ini menjadi salah satu penyebab terhambatnya upgrading sistem audit dan evaluasi yang dilakukan.

### **Kampanye dan Sosialisasi**

Tidak hanya tenaga kesehatan yang bersangkutan, namun pasien juga harus diberikan sosialisasi terkait data pribadi yang diberikan baik siapa saja yang bisa mengakses, transparansi penggunaan data medis hingga penyimpanan data tersebut. Rumah sakit harus membuat sebuah platform pengaduan pasien, agar ketika terjadi pelanggaran terkait data pribadi pasien bisa segera dilaporkan dan dapat juga bisa segera ditindaklanjuti dengan baik (Widjaja et al., 2025). Penelitian yang dilakukan oleh Susilowati et al (2025) terkait edukasi penggunaan *E-Health* dimana hasil penelitian menunjukkan bahwa edukasi yang dilakukan dari brosur perlindungan data diri pasien, masyarakat lebih memahami terkait pentingnya menjaga kerahasiaan password aplikasi dan pentingnya menyimpan data Riwayat kesehatan pribadi dengan baik. Peningkatan pengetahuan masyarakat terkait perlindungan data diri ini dapat membekali masyarakat dalam melakukan perlindungan efektif terhadap data diri yang ia miliki dan menghindari potensi ancaman sehingga tidak terjadi pelanggaran penyebaran data.

Strategi perlindungan data diri pasien yang dilakukan tidak hanya mencakup penguatan dari sisi keamanan teknologi saja, namun juga harus disertai dengan penguatan dari sisi edukasi pada tenaga kesehatan dan non kesehatan yang terlibat. Teknologi yang canggih tidak akan berdampak secara signifikan jika tidak disertai dengan adanya pengetahuan dan kesadaran etik profesional dari tenaga kesehatan dan non kesehatan yang terlibat. Efektivitas perlindungan data harus dilakukan dengan berbagai macam pendekatan antara teknologi dan edukasi yang berkelanjutan. Oleh karena itu, integrasi antara penguatan sistem teknologi dan penguatan pengetahuan terkait etik profesional menjadi poin penting dalam terlaksananya perlindungan data diri pasien secara menyeluruh dan layak. Tindakan ini juga sebagai cerminan dari tanggung jawab perawat dalam memberikan asuhan keperawatan yang aman serta strategi yang dilakukan juga dapat meningkatkan kepercayaan pasien terhadap pemberi pelayanan kesehatan.

## **4. KESIMPULAN**

Perlindungan data pribadi pasien merupakan sebuah dasar utama dalam menjaga kepercayaan masyarakat terhadap pelayanan kesehatan. Tenaga kesehatan bertanggung jawab secara hukum dan etik untuk menjaga kerahasiaan data pasien. Jika kerahasiaan medis disebar, hal itu dapat berdampak negatif pada hukum, etika profesi, dan kepercayaan publik terhadap layanan kesehatan.

Penelitian ini menyimpulkan bahwa strategi perlindungan data pasien yang efektif meliputi peningkatan sistem teknologi, edukasi berkelanjutan, audit dan evaluasi sistem serta sosialisasi. Implementasi prinsip etik confidentiality tidak hanya menjalankan kewajiban saja, namun juga sebagai bentuk upaya perlindungan data diri pasien selama proses perawatan. Regulasi perlindungan data pribadi pasien sudah ada di Indonesia, namun dalam pelaksanaannya belum optimal dan masih perlu banyak ditingkatkan agar data diri pasien terjaga dengan baik. Penelitian lanjutan dapat dilakukan untuk mengkaji lebih dalam terkait implementasi empat strategi ini dalam pelayanan kesehatan untuk memperkuat perlindungan data diri pasien secara digital.

## DAFTAR PUSTAKA

- Alanazi, A. (2025). *Assessing Clinicians' Legal Concerns and the Need for a Regulatory Framework for AI in Healthcare: A Mixed-Methods Study*. 1–15. <https://doi.org/10.3390/healthcare13131487>
- Alisa A, Yogi P, F. P. (2024). Melindungi Data di Dunia Digital : Peran Strategis Enkripsi Dalam Keamanan Data. *Journal of Scientech Research and Development*, 6(2), 540–549. <https://doi.org/10.56670/jsrd.v6i2.608>
- Febrianto et al., (2024). Studi Literatur: Landasan Dalam Memilih Metode Penelitian Yang Tepat. *Journal Educational Research and Development | E-ISSN: 3063-9158*, 1(2), 259–263. <https://doi.org/10.62379/jerd.v1i2.142>
- Ardianto, E. T., & Nurjanah, L. (2024). Analisis Aspek Keamanan Data Pasien Dalam. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, 3(2), 18–30. <https://rammik.pubmedia.id/index.php/rmik/article/view/54%0Ahttps://rammik.pubmedia.id/index.php/rmik/article/download/54/20>
- Beauchamp, T., & Childress, J. (2019). Principles of Biomedical Ethics: Marking Its Fortieth Anniversary. *American Journal of Bioethics*, 19(11), 9–12. <https://doi.org/10.1080/15265161.2019.1665402>
- Budiman, et al. (2025). Analisis Resiko dan Tindakan Pencegahan Kebocoran data Rekam Medis Elektronik Pasien di RS P Surakarta. *Journal of Multidisciplinary Research and Development Volume 7 Nomor 3* : 2118-2127. <https://doi.org/10.38035/rj.v7i3.1421>
- Candra et al. (2025). Perlindungan Data Pribadi Dalam Mencegah Tindak Pidana Penyalahgunaan Hak Pasien. *Jurnal Pendidikan dan Pengajaran*, Volume 6 Nomor 2 : 32-45.
- Chen, P., et al., (2026). *Protecting Radiology Data and Devices Against Cybersecurity Threats: A Joint White Paper of the ACR and Society for Imaging Informatics in Medicine 1*. <https://doi.org/10.1016/j.jacr.2025.07.014>
- Handayani, D. (2024). Evaluasi Pelaksanaan Hak Privasi Data Medis Pasien di Rumah Sakit. *Jurnal Evaluasi Kesehatan Indonesia*, 3(2), 88–102. <https://doi.org/10.55513/jeki.v3i2.88>
- Indiastari, D., Rosandy, K. O., Fajar, J. K., Rosandy, M. G., Sutanto, H., Candradikusuma, D., & Budiarti, N. (2023). Serba-serbi Terapi Anti Retroviral. *Serba-Serbi Terapi Anti Retroviral*, 11(April), 71–83. <https://doi.org/10.11594/ubpress9786232968455>
- Jiang, X., et al. (2023). *Professional Ethics and Safety Culture in Modern Healthcare Management*. *Frontiers in Public Health*, 11
- Kaendo, K, E, G & Ade, A. (2025). Comparison of The Right to Be Forgotten Regulations in Indonesia and European Union Countries. *Rechtidee*, 19(No 1), 106–117.
- Kasad, N. W. R. (2023). *Data Security Management and Audit of Healthcare Data: A Case Study of SISPEC19 Project*. 1(01). <https://doi.org/10.61973/apjisd.v101.4>
- Lestari, A. P., & Rohman, H. (2025). Keamanan Sistem Rekam Medis Elektronik Untuk Menjamin Privasi Pasien Di Rumah Sakit. *International Journal of Health and Information System*, 2(2)
- Lubis, et al. (2024). Legal Protection of Patient Data Privacy In Health Services At Regional General Hospitals Cut Meutia North Aceh. *International Conference Epicentrum of Economic Global Framework*, 212–224. <https://proceeding.pancabudi.ac.id/index.php/ICEEGLOF/issue/view/9>
- Munandar et al., (2022). *Etika dan Komunikasi Keperawatan*. Bandung : Media Sains Indonesia
- Mocydlarz et al., (2023). *Management of Onsite and Remote Communication in Oncology Hospitals: Data Protection in an Era of Rapid Technological Advances*. DOI 10.3390/jpm13050761



- Natamiharja, et all. (2024). Penguatan Kesadaran Masyarakat Terhadap Perlindungan data Pribadi di Era Digital. *Jurnal Hukum Pengabdian Kepada Masyarakat*, 3(2).
- Nurjanah, N. E., & Mukarromah, T. T. (2021). Pembelajaran Berbasis Media Digital Pada Anak Usia Dini Di Era Revolusi Industri 4.0 : Studi Literatur. *Jurnal Ilmiah Potensia*, 6(1), 66–77. <https://doi.org/10.33369/jip.6.1>.
- Pradana, Yudha Aditya dan Wilma Silalahi. (2024). Implementasi dan Tantangan Regulasi Perlindungan Data Pribadi Pasien di Era Digital Pada Rumah Sakit. *Jurnal Hukum Lex Generalis* Volume 5 No 12 : hal 1-13. <https://doi.org/10.56370/jhlg.v5i12.1329>
- Saputra, Tri Eka. (2023). Penggunaan Rekam Medis Elektronik dalam Mewujudkan Perlindungan Hukum Keamanan Data Pribadi Pasien. *Jurnal Ilmiah Hukum* Volume 13 Nomor 2 : 57-75. DOI : 10.34303
- Schmitt, T. (2023). *Implementing Electronic Health Records in Germany : Lessons ( Yet to Be ) Learned*. 23(1), 1–13. <https://doi.org/10.5334/ijic.6578>
- Semyonov-tal, K. (2024). *Keeping medical information safe and confidential : a qualitative study on perceptions of Israeli physicians*. 9, 1–10. DOI 10.1186/s13584-024-00641-9
- Shakila, Ramilla & Ayu Hendrati Rahayu. (2025). Tinjauan Perlindungan Hak Akses Terhadap Data Pasien Dalam Rekam Medis Elektronik di RSUD Cililin. *Jurnal Kesehatan Tambusai* Volume 6 Nomor 3, 10858 - 10866. <https://doi.org/10.31004/jkt.v6i3.48971>
- Sofia et all. (2022). Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, 1(2), 94–103. <https://doi.org/10.47134/rmik.v1i2.29>
- Subramanian, H., Sengupta, A., & Xu, Y. (2024). *Patient Health Record Protection Beyond the Health Insurance Portability and Accountability Act : Mixed Methods Study Corresponding Author : 26*. <https://doi.org/10.2196/59674>
- Susilowati, et all. (2025). Edukasi Mengenai Upaya Menjaga Privasi Data Pribadi Dalam Penggunaan E-Health. *Journal of Community Engagement and Empowement*, 7(1), 63–69.
- Widjaja, et al. (2025). Peran Rumah Sakit Sebagai Pengendali Data Dalam Menjamin Keamanan Data Pribadi Pasien Pada Sistem Kesehatan Digital. *Jurnal Kesehatan*, Vol 3 No 2, Hal 159-167. <https://doi.org/10.58936/jk.v3i2.559>

#### **Sumber Hukum dan Non Akademik**

- Permenkes Nomor 36 Tahun 2012 diakses dari <https://peraturan.go.id/files/bn915-2012.pdf> pada tanggal 23 Oktober 2025
- Pos Kota. (2025). Viral! Pegawai Asuransi Dipecat Usai Sebar Data Medis dan Remehkan Penyakit Dara Arafah, Ini Akun IG Nadia Venika <https://www.poskota.co.id/2025/07/10/viral-pegawai-asuransi-dipecat-usai-sebar-data-medis-dan-remehkan-penyakit-dara-arafah-ini-akun-ig-nadia-venika>
- Undang-Undang (UU) Nomor 27 tahun 2022 Tentang Perlindungan Data Pribadi diakses dari <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>

**Halaman ini dikosongkan**