



Studi Literatur: Analisis Keamanan dan Privasi Data Rekam Medis Elektronik Fasilitas Pelayanan Kesehatan Berdasarkan UU Nomor 27 Tahun 2022

Adelia Ingrid Putri Maharani^{1*}, Sinta Novratilova², Azalia Tjandra Dewi³, Dwi Rena Aulia⁴, Rina Wulandari⁵, Aldi Juli Saputra⁶

¹⁻⁶Program Studi Sarjana Terapan Manajemen Informasi Kesehatan, Politeknik Indonusa Surakarta, Indonesia

*Penulis Korespondensi: adeliaingridputrimaharani@gmail.com

Abstract. Systemic non-compliance with PERMENKES 24/2022 & UU PDP 27/2022 on EHR, such as human error, weak passwords, vulnerable physical access, and low ISO 27001, increases the risk of data breaches & fines. This research fills the gap in the study by evaluating the compliance of the CIA Triad principles on Electronic Medical Records post-issuance of PERMENKES No. 24 of 2022 and Law No. 27 of 2022 thru a literature review, while also highlighting the impact of non-compliance on service quality and patient trust. This study aims to evaluate the compliance of healthcare facility security systems with PERMENKES No. 24 of 2022 and Law No. 27 of 2022 and analyze the impact of non-compliance on service quality and patient trust. This research method employs a systematic narrative literature review design to comprehensively examine the implementation of the CIA Triad in EHR security. Searches were conducted on Google Scholar (2023-2026) using the keywords "data security and privacy," "electronic medical records," and "CIA Triad." The research results show that all four healthcare facilities have adopted access control, TTE, VPN, encryption, and SSL/TLS in accordance with PERMENKES No. 24/2022 and Article 35 of the PDP Law No. 27/2022. However, the effectiveness is hindered by authentication weaknesses (weak passwords, long auto logout), the absence of written SOPs, low staff compliance, and minimal patient socialization, resulting in the data subject's rights not being transparently fulfilled. The lack of data security socialization to patients indicates that transparency and protection of data subjects' rights based on Law No. 27 of 2022 are not optimal.

Keywords: CIA Triad; Data Security; EMR; PDP Law; Privacy.

Abstrak. Ketidakpatuhan sistemik PERMENKES 24/2022 & UU PDP 27/2022 pada RME seperti *human error*, *password* lemah, akses fisik rentan, ISO 27001 rendah meningkatkan risiko kebocoran data & sanksi denda. Penelitian ini mengisi kekosongan kajian dengan mengevaluasi kesesuaian prinsip *CIA Triad* pada Rekam Medis Elektronik pasca-penerbitan PERMENKES No. 24 Tahun 2022 dan UU No. 27 Tahun 2022 melalui *literature review*, serta menyoroti dampak ketidakpatuhan terhadap mutu pelayanan dan kepercayaan pasien. Penelitian ini bertujuan untuk mengevaluasi kesesuaian sistem keamanan fasilitas kesehatan terhadap PERMENKES Nomor 24 Tahun 2022 dan Undang-Undang Nomor 27 Tahun 2022 serta menganalisis dampak ketidakpatuhan terhadap mutu pelayanan dan tingkat kepercayaan pasien. Metode penelitian ini menerapkan desain *literature review* naratif sistematis untuk mengkaji komprehensif implementasi *CIA Triad* pada keamanan RME. Pencarian di *Google Scholar* (2023-2026) dengan kata kunci "keamanan dan privasi data", "rekam medis elektronik", serta "*CIA Triad*". Hasil penelitian menunjukkan bahwa keempat fasilitas kesehatan telah mengadopsi kontrol akses, TTE, VPN, enkripsi, dan SSL/TLS sesuai PERMENKES No. 24/2022 serta Pasal 35 UU PDP No. 27/2022. Namun, efektivitas terhambat oleh kelemahan autentikasi (*password* lemah, *auto logout* lama), absennya SOP tertulis, rendahnya kepatuhan staf, dan minimnya sosialisasi pasien, sehingga hak subjek data belum terpenuhi secara transparan. Kurangnya sosialisasi keamanan data kepada pasien menandakan bahwa transparansi dan perlindungan hak subjek data berdasarkan UU No. 27 Tahun 2022 belum optimal.

Kata kunci: *CIA Triad*; Keamanan Data; Privasi; RME; UU PDP.

1. LATAR BELAKANG

Transisi menuju rekam medis elektronik bukan sekadar kewajiban teknis, melainkan pertarungan besar antara kepatuhan hukum yang ketat dan reputasi layanan kesehatan di mata publik. Peraturan Menteri Kesehatan No. 24 Tahun 2022 mewajibkan seluruh fasilitas pelayanan kesehatan untuk menyelenggarakan rekam medis secara elektronik dan terintegrasi dengan platform SATUSEHAT menggunakan standar HL7 FHIR. Kebijakan ini mewajibkan penerapan enkripsi AES-256, kontrol akses berbasis peran (RBAC), *backup* harian, serta audit log demi menjamin kerahasiaan, integritas, dan ketersediaan data pasien sesuai *CIA Triad* (Nurul Fajriah Istiqamah 2025). Sejalan dengan hal tersebut, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengklasifikasikan data kesehatan sebagai data spesifik yang memerlukan persetujuan eksplisit tertulis, enkripsi tingkat tinggi, dan *pseudonymisation*.

Fasilitas kesehatan selaku pengendali data wajib melaporkan kebocoran dalam waktu 72 jam kepada otoritas PDP, menunjuk *Data Protection Officer* (DPO), dan melakukan *Data Protection Impact Assessment* (DPIA) tahunan, di mana pelanggaran data medis dapat dikenai sanksi administratif hingga pidana enam tahun penjara serta denda Rp6 miliar. Namun, temuan di lapangan seperti di RSP Surakarta (2025) dan RSUD Waras Wiris Boyolali (2025) menunjukkan masih terjadi *human error*, akses fisik yang tidak terjaga, kerentanan peretasan, duplikasi nomor rekam medis, serta peminjaman akun petugas yang melanggar ketentuan PDP dan standar ISO 27001. Penelitian di RSUD Waras Wiris Boyolali mengevaluasi *CIA Triad* secara kualitatif melalui wawancara dan observasi. Temuan utama meliputi ancaman *confidentiality* akibat penggunaan *password* bersama serta kerusakan *integrity* dari duplikasi nomor RM, meskipun ketersediaan terjamin dengan *backup* berkala. Pelanggaran prinsip juga ditemukan di RSI Sultan Agung (2025), melaporkan sebanyak 73% petugas gagal menerapkan enkripsi dengan tingkat kepatuhan ISO 27001 hanya 49% dari 108 klausul, di mana akses tidak sah menjadi temuan dominan. Penelitian di Rumah Sakit PKU Muhammadiyah Wonogiri Kota (2023) mengungkapkan bahwa keamanan terhadap kerahasiaan rekam medis sangat bergantung pada fasilitas ruang penyimpanan (*filing*) yang memadai, termasuk perlindungan dari aspek fisik, biologi, dan kimiawi. Temuan tersebut menyoroti kerentanan seperti absennya fasilitas *fingerprint* pada pintu ruang *filing* yang hanya menggunakan kunci biasa, serta adanya akses petugas non-rekam medis ke area sensitif tersebut.

Kemudian dilakukan analisis mendalam menggunakan teknik *literature review* mengenai keamanan dan privasi data pada beberapa fasilitas pelayanan kesehatan ditemukan adanya *ransomware*, *phishing*, dan *human error* sebagai ancaman utama dengan solusi biometrik dan AI deteksi intrusi (Ikawati, Ansyori, and Permatasari 2025). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi landasan hukum utama yang mewajibkan fasilitas kesehatan sebagai pengendali data untuk menerapkan enkripsi tingkat tinggi, audit log, dan pelaporan kebocoran data dalam 72 jam kepada otoritas.

Fenomena sistemik ini mengancam sanksi bagi fasilitas kesehatan yang tidak patuh. Penelitian sebelumnya oleh di RSUD Waras Wiris Boyolali (2025) umumnya hanya meninjau kepatuhan terhadap PERMENKES, sehingga terdapat kekosongan kajian mengenai dampak penerapan kedua regulasi tersebut terhadap kualitas pelayanan dan kepercayaan pasien. Kebaruan penelitian ini terletak pada analisis keamanan dan privasi data pasien pasca-pemberlakuan PERMENKES No. 24 Tahun 2022 dan UU No. 27 Tahun 2022. Dengan demikian, penelitian ini bertujuan untuk mengevaluasi kesesuaian sistem keamanan fasilitas kesehatan terhadap kedua dasar hukum tersebut serta menilai dampak ketidakpatuhan terhadap mutu pelayanan dan tingkat kepercayaan pasien. Tingkat kepatuhan fasilitas kesehatan terhadap PERMENKES No. 24 Tahun 2022 dan UU PDP berkorelasi langsung dengan efektivitas CIA Triad dalam RME. Implementasi keamanan rendah meningkatkan risiko kebocoran data serta mengganggu kontinuitas pelayanan. Hal ini juga menurunkan akses data dan kepercayaan pasien terhadap sistem digital kesehatan nasional.

2. KAJIAN TEORITIS

Rekam medis elektronik (RME) didefinisikan sebagai rekam medis yang dibuat, disimpan, ditampilkan, diedit, ditransmisikan, dan dipindahkan melalui sistem elektronik (PERMENKES Nomor 24 Tahun 2022). Pada peraturan tersebut mewajibkan setiap fasilitas pelayanan kesehatan menyediakan RME terintegrasi dengan platform SATUSEHAT untuk akses data pasien lintas layanan, menggantikan rekam medis manual yang rentan kehilangan, duplikasi data, dan kesulitan akses antar fasilitas. Integrasi ini memastikan data pasien terkoordinasi secara nasional melalui SATUSEHAT portal, sebagaimana diatur dalam Pasal 3 yang menekankan implementasi penuh termasuk enkripsi, *backup* handal, dan pelacakan perangkat seperti IMEI untuk tenaga medis.

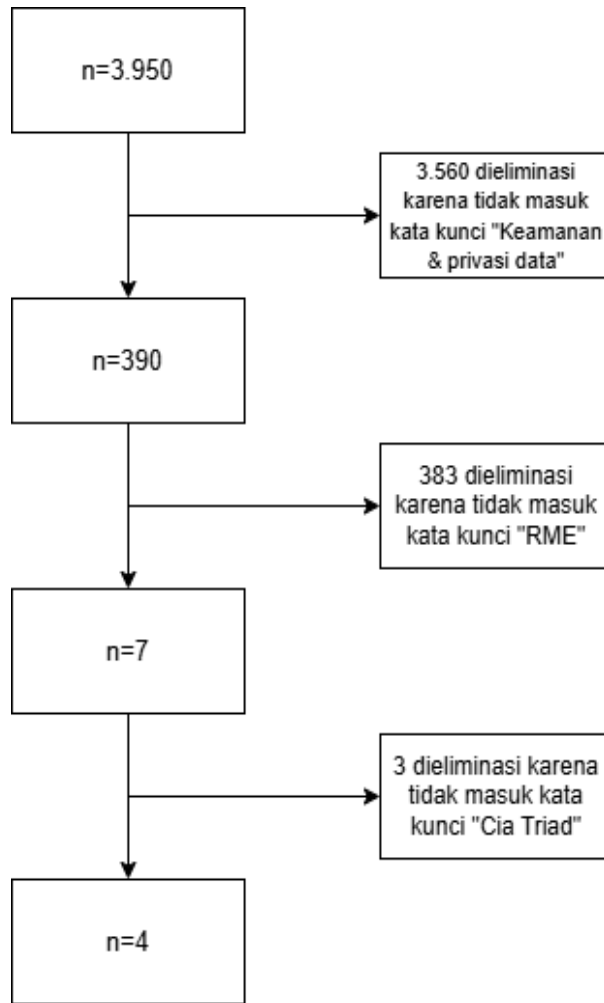
RME harus mematuhi prinsip *CIA Triad* dari buku Prinsip Inti Keamanan Informasi karya Yunmar et al. (2026), yaitu *Confidentiality* (kerahasiaan melalui enkripsi *end-to-end* dan autentikasi multi-faktor), *Integrity* (integritas melalui *hash validation* dan *audit trail*), serta *Availability* (ketersediaan melalui redundansi server dan *disaster recovery plan*). PERMENKES No. 24 tahun 2022 pada pasal 29 secara eksplisit mewajibkan penerapan prinsip ini untuk mencegah akses tidak sah, kebocoran, atau manipulasi data pasien. Fasilitas kesehatan diwajibkan menerapkan audit trail otomatis yang mencatat setiap perubahan, termasuk siapa, apa, dan kapan modifikasi dilakukan sebagai lapisan perlindungan tambahan.

UU Perlindungan Data Pribadi (PDP) No. 27 Tahun (2022) menjadi fondasi krusial bagi sektor kesehatan, mengharuskan fasilitas memperoleh persetujuan tertulis pasien sebelum mengumpulkan, menggunakan, atau mengungkapkan data pribadi, serta memberikan hak penarikan persetujuan kapan saja. Undang-undang ini mencegah penyalahgunaan data di era digital seperti pada RME dan telemedicine, dengan sanksi tegas bagi pelanggar, meskipun tantangan infrastruktur lemah masih perlu diatasi melalui peraturan pelaksana yang lebih kuat. Prinsipnya selaras dengan standar internasional seperti GDPR dan HIPAA, memperkuat akuntabilitas fasilitas pelayanan kesehatan dalam menjaga privasi pasien.

3. METODE PENELITIAN

Penelitian ini menggunakan desain *literature review* naratif yang sistematis untuk mengkaji secara komprehensif implementasi *CIA Triad* dalam keamanan Rekam Medis Elektronik (RME). *Literature review* merupakan metode penelitian yang bertujuan untuk mengidentifikasi, mengevaluasi, dan mensintesis hasil penelitian yang telah dipublikasikan guna memperoleh gambaran yang lebih menyeluruh mengenai suatu topik tertentu.

Kami menggunakan *Google Scholar* periode (tahun 2023-2026) dengan kata kunci utama "keamanan dan privasi data". Tahap kedua menggunakan "rekam medis elektronik". Tahap ketiga menggunakan kata kunci "*CIA Triad*". Setelah ditelaah dan diambil artikel yang termasuk dalam inklusi yaitu artikel yang berbahasa Indonesia dan berupa artikel ilmiah, maka hanya tersisa 4 artikel.



Gambar 1. Alur Penelitian

4. HASIL DAN PEMBAHASAN

HASIL

Berdasarkan hasil pencarian artikel menggunakan kata kunci pada *database Google Scholar* yang diperoleh dari internet, populasi penelitian ini yaitu seluruh artikel nasional yang berkaitan dengan topik keamanan dan privasi data kesehatan, rekam medis elektronik, serta prinsip *CIA Triad*. Sedangkan sampelnya yaitu artikel yang memenuhi kriteria inklusi berupa artikel kajian (*review articles*) dengan tahun terbit 2023-2026.

Tabel 1. Hasil Identifikasi dan Seleksi Artikel.

No.	Judul	Tahun	Aspek Keamanan	Kekurangan
1	Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso	2025	Setiap pengguna memiliki <i>username/password</i> individual dengan manajemen terpusat (kepala RM & IT); perubahan <i>password</i> 3 bulan sekali; auto <i>logout</i> ; akses terbatas per <i>role</i> dengan edit maksimal 24 jam; perubahan besar hanya admin; data tak bisa diubah sembarangan; ketersediaan dijamin genset; internet stabil; <i>database</i> dinas/infokes; retensi 25 tahun.	<i>Auto logout</i> masih kurang optimal (bisa sampai ± 1 jam setelah aktivitas). Belum disebutkan adanya enkripsi atau 2FA.
2	Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X	2024	Sistem menggunakan <i>username/password</i> per pengguna; auto <i>logout</i> 30 menit; edit data sesuai hak akses (dokter 24 jam); TTE tersertifikasi dengan kode autentikasi dokter; akses hanya via jaringan internal/VPN IT dengan hak akses spesifik berdasarkan peran.	Belum ada kewajiban penggantian <i>password</i> berkala; minimnya penggunaan karakter khusus; ketiadaan SOP khusus keamanan data; sistem tidak menyediakan fitur penghapusan data untuk menjaga riwayat medis pasien; proses tanda tangan pasien masih manual.
3	Pelaksanaan Rekam Medis Elektronik di Rumah Sakit Islam Jakarta Sukapura	-	Sistem menerapkan <i>role-based access control</i> oleh tim IT; hanya unit terkait yang dapat <i>input/edit</i> data; didukung TTE dokter; jaringan internet/server terkelola IT; akses terintegrasi antar unit (perawat, dokter, farmasi, kasir); fitur log mencatat identitas pengguna, <i>timestamp</i> , dan tindakan (<i>input/edit/lihat</i> data).	Terdapat kelalaian/pelanggaran oleh petugas; belum adanya SOP tertulis yang spesifik mengatur penggantian <i>password</i> rutin.
4	Keamanan Sistem Rekam Medis Elektronik Untuk Menjamin Privasi Pasien Di Rumah Sakit Mitra Idaman Kota Banjar	2025	Sistem menerapkan <i>username/password</i> kuat unik per individu; enkripsi data; audit trail ketat untuk deteksi manipulasi; backup rutin; keamanan <i>jaringan</i> menggunakan protokol SSL/TLS; ruang server dijaga fisik; mekanisme khusus menangani perubahan/penghapusan data oleh administrator.	Kurangnya pelaporan insiden keamanan secara konsisten; tingkat kepatuhan rendah terhadap kebijakan keamanan data; kurangnya transparansi kepada pasien; minimnya sosialisasi aspek keamanan yang menurunkan kepercayaan pasien.

Sistem keamanan rekam medis di UPT Puskesmas Karangploso (2025) telah menerapkan kontrol akses berbasis peran (*role-based access*) dan manajemen kata sandi berkala untuk menjaga kerahasiaan data. Aspek ketersediaan juga terjamin melalui infrastruktur cadangan seperti genset dan retensi data hingga 25 tahun. Namun, efektivitas sistem ini masih terhambat oleh durasi auto *logout* yang terlalu lama (mencapai 60 menit) serta

absennya fitur enkripsi dan autentifikasi dua faktor (2FA). Celah ini sangat berisiko bagi keamanan data pasien jika perangkat ditinggalkan tanpa pengawasan dalam waktu lama.

Sistem di Rumah Sakit X (2024) telah memperkuat autentifikasi melalui Tanda Tangan Elektronik (TTE) tersertifikasi dan pembatasan akses jaringan via VPN. Meski fitur *auto logout* 30 menit sudah berjalan, keamanan akun masih rentan karena tidak adanya kewajiban ganti *password* berkala maupun penggunaan karakter khusus. Selain itu, tata kelola data belum sepenuhnya digital karena ketiadaan SOP keamanan khusus dan proses tanda tangan pasien yang masih manual menggunakan kertas.

Sistem Rekam Medis Elektronik (RME) di Rumah Sakit Islam Jakarta Sukapura (2024) telah menerapkan kontrol akses berbasis jabatan (*role-based access control*) dan fitur log untuk memantau setiap aktivitas pengguna secara rinci. Meskipun didukung oleh Tanda Tangan Elektronik (TTE) dan integrasi antar unit yang baik, keamanan sistem ini masih terancam oleh penggunaan kata sandi yang sederhana. Kelemahan utama terletak pada jarangya penggantian kata sandi serta ketiadaan SOP tertulis yang secara spesifik mengatur prosedur keamanan akun bagi petugas.

RS Mitra Idaman Kota Banjar (2025) telah memperkuat teknis keamanan melalui enkripsi data, protokol SSL/TLS, dan pengawasan fisik ruang server. Meskipun sistem backup dan perlindungan data sudah berjalan, efektivitasnya terhambat oleh rendahnya kepatuhan staf dan tidak konsistennya pelaporan insiden keamanan. Selain itu, minimnya sosialisasi kepada pasien mengenai aspek keamanan informasi berisiko menurunkan transparansi serta kepercayaan publik terhadap layanan rumah sakit.

Secara keseluruhan, keempat fasilitas kesehatan telah menerapkan kontrol akses berbasis peran dan penguatan infrastruktur teknis seperti VPN, SSL/TLS, hingga Tanda Tangan Elektronik untuk menjaga keamanan data. Namun, efektivitas sistem ini masih terkendala oleh manajemen autentikasi yang lemah (seperti kata sandi sederhana dan durasi *auto logout* yang lama), rendahnya kepatuhan staf dalam prosedur keamanan berkala, serta ketiadaan SOP tertulis yang spesifik. Selain itu, ketergantungan pada proses manual dan minimnya sosialisasi keamanan kepada pasien menunjukkan bahwa aspek privasi serta tata kelola digital di sektor ini masih memerlukan standar operasional yang lebih ketat dan transparan.

PEMBAHASAN

Mengenai aspek keamanan dan privasi di keempat fasilitas kesehatan ini menunjukkan upaya adaptasi terhadap standar regulasi digital, namun dengan tingkat keberhasilan yang bervariasi dalam praktiknya. UPT Puskesmas Karangploso telah mengawali langkah kepatuhan terhadap PMK No. 24 Tahun 2022 dengan menerapkan *role-based access control* dan manajemen kata sandi berkala untuk menjamin kerahasiaan rekam medis. Infrastruktur pendukung seperti genset dan retensi data 25 tahun di sana pun telah selaras dengan prinsip ketersediaan dalam Pasal 35 UU PDP, meskipun efektivitasnya masih terganjal oleh sistem *auto logout* yang mencapai 60 menit sehingga berisiko mengundang akses tidak sah.

Rumah Sakit X mengimplementasikan standar autentikasi yang kuat sesuai Pasal 31 PMK No. 24 Tahun 2022 dengan menggunakan Tanda Tangan Elektronik (TTE) tersertifikasi dan pembatasan jaringan melalui VPN IT. Meskipun telah memiliki fitur *auto logout* selama 30 menit, rumah sakit ini masih menghadapi tantangan dalam memenuhi kewajiban organisasi sesuai Pasal 39 UU PDP karena belum adanya SOP khusus keamanan data dan proses administrasi pasien yang masih manual menggunakan kertas. Selain itu, ketiadaan kewajiban ganti *password* berkala dan minimnya penggunaan karakter khusus menunjukkan bahwa perlindungan akun pengguna belum sepenuhnya optimal sesuai standar privasi digital.

RS Islam Jakarta Sukapura telah memenuhi prinsip akuntabilitas UU PDP melalui fitur log yang mencatat aktivitas pengguna secara mendetail. Sinergi antara penggunaan TTE dokter dan integrasi data lintas unit juga menunjukkan kepatuhan terhadap standar sistem terpadu pada PMK No. 24 Tahun 2022. Namun, kerahasiaan data masih rentan akibat penggunaan kata sandi sederhana dan jarangunya pembaruan akun, yang diperburuk oleh absennya SOP tertulis mengenai protokol keamanan rutin bagi petugas.

RS Mitra Idaman Kota Banjar menunjukkan kepatuhan teknis yang paling menonjol terhadap Pasal 35 UU PDP melalui penerapan enkripsi data, penggunaan protokol SSL/TLS, serta pengamanan fisik pada ruang server. Meski sistem *backup* rutin telah berjalan sesuai standar perlindungan data rekam medis, efektivitasnya masih terhambat oleh rendahnya kepatuhan staf dan tidak konsistennya pelaporan insiden keamanan. Selain itu, minimnya sosialisasi keamanan informasi kepada pasien berisiko menurunkan transparansi dan kepercayaan publik, yang merupakan elemen penting dalam menjaga hak subjek data sesuai dengan ketentuan undang-undang perlindungan data pribadi.

Secara keseluruhan, keempat faskes telah mengadopsi kontrol akses dan Tanda Tangan Elektronik (TTE) sesuai PMK No. 24 Tahun 2022. Penggunaan VPN, enkripsi, dan protokol SSL/TLS juga menunjukkan kepatuhan teknis terhadap Pasal 35 UU PDP. Namun, efektivitasnya terhambat oleh *password* yang lemah, *auto logout* yang terlalu lama, dan absennya SOP tertulis. Selain itu, rendahnya kepatuhan staf dan minimnya sosialisasi keamanan kepada pasien masih menjadi kendala utama dalam memenuhi hak subjek data secara transparan sesuai mandat UU No. 27 Tahun 2022.

Ketidakpatuhan terhadap standar keamanan dan privasi data kesehatan menurut UU PDP berisiko menimbulkan sanksi administratif atau pidana bagi fasilitas kesehatan (Kathleen, Kalaringga, and Prasetyo 2025). Selain itu, hal ini menurunkan akses data bagi tenaga medis dan pasien, sehingga menghambat layanan kesehatan digital nasional. Kebocoran data berulang juga merusak kepercayaan pasien pada sistem RME, menekan adopsi teknologi kesehatan, meningkatkan ketergantungan proses manual, dan melemahkan transformasi digital sektor kesehatan Indonesia.

5. KESIMPULAN DAN SARAN

Kesimpulan

Keempat fasilitas kesehatan telah berupaya memenuhi standar PMK No. 24 Tahun 2022 melalui penerapan kontrol akses berbasis peran (*role-based access*) dan penggunaan Tanda Tangan Elektronik (TTE). Kepatuhan teknis terhadap Pasal 35 UU PDP juga terlihat pada penggunaan enkripsi, SSL/TLS, serta VPN untuk melindungi data rekam medis. Namun, efektivitas keamanan masih terhambat oleh manajemen akun yang lemah (kata sandi sederhana dan durasi *auto logout* yang lama), ketiadaan SOP tertulis yang spesifik, serta rendahnya kepatuhan operasional staf. Selain itu, minimnya sosialisasi keamanan kepada pasien menunjukkan bahwa transparansi dan perlindungan hak subjek data sesuai UU No. 27 Tahun 2022 belum tercapai secara optimal.

Saran

Untuk mencapai kepatuhan penuh sesuai standar nasional dan menjamin privasi data pasien, fasilitas kesehatan disarankan untuk: (1) Menerapkan verifikasi dua langkah (2FA) dengan menambah lapisan keamanan akses selain hanya mengandalkan kata sandi. Membuat panduan tertulis (SOP) yang tegas mengenai prosedur penggunaan sistem dan pelaporan insiden; (2) Memberikan edukasi privasi dan keamanan digital bagi seluruh staf untuk mengubah perilaku kerja; (3) Melakukan audit trail jejak akses memastikan adanya akuntabilitas, sehingga jika terjadi kebocoran, fasyankes dapat melacak siapa yang

bertanggung jawab; (4) Menjamin integritas data dengan penggunaan tanda tangan elektronik agar tidak diubah oleh pihak yang tidak berwenang, sehingga autentisitas informasi medis tetap terjaga sepanjang siklus pelayanan kesehatan sesuai mandat UU PDP.

DAFTAR REFERENSI

- Ardianto, Efri Tri, Sabran, and Lensa Nurjanah. 2024. "Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X." *RAMMIK : Jurnal Rekam Medik Dan Manajemen Informasi Kesehatan* Vol. 3(2):18–30. doi: <https://doi.org/10.47134/rammik.v3i2.54>.
- Budiman, Arief, Muzakar Isa, and Siti Soekiswati. 2025. "Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RS P Surakarta." *Ranah Research (Journal of Multidisciplinary Research and Development)* 7(3):2118–27. doi: <https://doi.org/10.38035/rj.v7i3>.
- Ekasari, Diah Devita. 2025. "Tinjauan Keamanan Data Dan Informasi Dalam Penyelenggaraan Rme Berdasarkan Permenkes No 24 Tahun 2022 Di Rsud Waras Wiris Boyolali." Universitas Duta Bangsa.
- Fahmi, Mochamad, Sri Sugiarsi, and Erna Adita Kusumawati. 2025. "Indonesian Journal of Health Information Management (IJHIM) Vol . 5 No . 2 (2025), 1 Keamanan Sistem Rekam Medis Elektronik Untuk Menjamin Privasi Pasien Di Rumah Sakit Mitra Idaman Kota Banjar Electronic Health Record System Security To Ensure Patient Privacy In Mitra Idaman Hospital Banjar City 2 | Indonesian Journal of Health Information Management (IJHIM), Vol . 5 No . 2 (2025),." 5(2):1–9.
- Ikawati, Fita Rusdian, Anis Ansyori, and Dewi Anggih Surya Permatasari. 2025. "Literature Review : Analisis Keamanan Data Rekam Medis Elektronik Di Fasilitas Kesehatan." *Manajemen Informasi Kesehatan* 10(2):230–37. doi: <https://doi.org/10.51851/jmis.v10i2.673>.
- Kathleen, Gabriella Aurel, Iga Kalaringga, and Boedi Prasetyo. 2025. "Pertanggungjawaban Rumah Sakit Atas Pelanggaran Pelindungan Data Pribadi Pasien Pasca Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat* 11(3):531–45. doi: <https://doi.org/10.55809/tora.v11i3.630>.
- Menteri Kesehatan Republik Indonesia. 2022. *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis*. Jakarta.
- Nurul Fajriah Istiqamah, Mujtahidah. 2025. "PERMENKES NO. 24/2022 DAN INTEROPERABILITAS REKAM MEDIS ELEKTRONIK." [https://jo\(24\):114–22](https://jo(24):114–22).
- Prayoga, Dina Ayu, Sinta Novratilova, and Wahyu Ratri Sukmaningsih. 2023. "Analisis Aspek Keamanan Ruang Filing Terhadap Kerahasiaan Dokumen Rekam Medis Di Rumah Sakit PKU Muhammadiyah Wonogiri Kota." *Journal Health Information Management Indonesian (JHIMI)* 02. doi: <https://doi.org/10.46808/jhimi.v2i2.147>.
- Presiden Republik Indonesia. 2022. *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. Indonesia.

- Rani, Destri Maya, and Bajeng Nurul Widyaningrum. 2025. "Evaluasi Keamanan Informasi Sistem Rekam Medis Elektronik Di RSI Sultan Agung." 10(<https://ojs.stikessaptabakti.ac.id/jmis/issue/view/67>):52–62. doi: <https://doi.org/10.51851/jmis.v10i1.636>.
- Suhariyono, Untung Slamet, Fita Rusdian Ikawati, and Nur Afifah. 2025. "Analisis Aspek Keamanan Informasi Data Pasien Pada Rekam Medis Elektronik Di UPT Puskesmas Karangploso." *Jurnal Manajemen Informasi Kesehatan Indonesia* 13(1):2337–2585.
- Wardani, Endah, Daniel Happy Putra, Dina Sonia, and Noor Yulia. 2024. "Keamanan Sistem Informasi Rekam Medis Elektronik Di Rumah Sakit Islam Jakarta Sukapura." *RAMMIK : Jurnal Rekam Medik Dan Manajemen Informasi Kesehatan Vol. 3(2)*:31–38. doi: <https://doi.org/10.47134/rammik.v3i2.1756>.
- Yunmar, Rajif Agung, Yendi Putra, Muhammad Irwan Syahib, Victor Lamboy Sinaga, Amna, Andi Muhammad Nur Hidayat, Muh. Hajar Akbar, and Jarot Budiasto. 2026. "Prinsip Inti Keamanan Informasi." P. 31 in *Keamanan Siber: Prinsip, Praktik, dan Pertahanan*, edited by H. Purnama. Padang: Get Press Indonesia.