

LITERATUR REVIEW TENTANG KEAMANAN DATA DAN PRIVASI DALAM REKAM MEDIS ELEKTRONIK DI INDONESIA

LITERATURE REVIEW ON DATA SECURITY AND PRIVACY IN ELECTRONIC MEDICAL RECORDS IN INDONESIA

Afrido^{1*}, Flora Aulia Islami², Khalisya Salma Tsabilla³, Layina Shahira⁴, Nafiarezkyy Aleifea⁵

^{1,2,3,4,5} Program Studi D3 Rekam Medis dan Informasi Kesehatan, Poltekkes Kemenkes Tasikmalaya, Cirebon.

Korespondensi e-mail: afridoido09@gmail.com

ABSTRAK

Perkembangan teknologi informasi di sektor kesehatan telah mendorong implementasi Rekam Medis Elektronik (RME) di Indonesia. Digitalisasi ini menawarkan efisiensi, integrasi, dan kemudahan akses, namun juga menghadirkan tantangan serius terkait keamanan data, privasi, dan aspek hukum. Artikel ini merupakan tinjauan literatur yang membahas tiga isu utama: aspek keamanan data, aspek privasi dan kerahasiaan, serta dasar hukum perlindungan rekam medis elektronik di Indonesia. Kajian dilakukan dengan menelaah berbagai penelitian, baik yang bersifat empiris di fasilitas kesehatan maupun kajian normatif terkait regulasi, termasuk Permenkes No. 24 Tahun 2022, Undang-Undang Perlindungan Data Pribadi (UU PDP), dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Hasil kajian menunjukkan bahwa penerapan keamanan data kesehatan masih menghadapi kelemahan pada aspek integritas, autentikasi, dan mekanisme audit meskipun telah mengadopsi standar seperti ISO 27001. Privasi pasien juga berisiko terganggu akibat rendahnya kesadaran SDM dan meningkatnya ancaman siber. Selain itu, implementasi dan penegakan regulasi di Indonesia masih menghadapi berbagai tantangan.

Kata kunci: Rekam Medis Elektronik, keamanan data, privasi, kerahasiaan, perlindungan data pribadi

ABSTRACT

The development of information technology in the health sector has encouraged the implementation of Electronic Medical Records (EMR) in Indonesia. This digitization offers efficiency, integration, and ease of access but also presents serious challenges related to data security, privacy, and legal aspects. This article is a literature review that discusses three main issues: data security aspects, privacy and confidentiality aspects, and the legal basis for the protection of electronic medical records in Indonesia. The study was conducted by examining various studies, both empirical studies in health facilities and normative studies related to regulations, including Minister of Health Regulation No. 24 of 2022, the Personal Data Protection Law (PDP Law), and the Electronic Information and Transaction Law (ITE Law). The findings indicate that the implementation of health data security continues to face challenges in terms of integrity, authentication, and audit mechanisms despite the adoption of international standards such as ISO 27001. Patient privacy also remains at risk due to limited human resource awareness and the increasing threat of cyberattacks. Furthermore, the implementation and enforcement of health data protection regulations in Indonesia continue to encounter significant challenges.

Keywords: *Electronic Medical Records, data security, privacy, confidentiality, personal data protection*

Pendahuluan

Transformasi digital dalam bidang kesehatan telah membawa perubahan fundamental terhadap cara penyedia layanan kesehatan menyimpan, mengelola, dan mendistribusikan informasi medis pasien. Salah satu inovasi penting adalah implementasi Rekam Medis Elektronik (RME) yang menggantikan pencatatan manual berbasis kertas. RME tidak hanya berfungsi sebagai sarana dokumentasi medis, melainkan juga sebagai instrumen pendukung pengambilan keputusan klinis, peningkatan mutu layanan, dan integrasi sistem informasi kesehatan lintas fasilitas.

Secara global, penerapan RME didorong oleh kebutuhan akan efisiensi, akurasi, dan interoperabilitas. Di Amerika Serikat, misalnya, *Health Information Technology for Economic and Clinical Health (HITECH) Act* telah mempercepat adopsi RME secara luas di rumah sakit dan klinik. Sementara di Uni Eropa, General Data Protection Regulation (GDPR) menetapkan standar ketat dalam perlindungan data pribadi, termasuk data kesehatan, sehingga aspek keamanan dan privasi menjadi prioritas utama dalam implementasi sistem informasi medis.

Di Indonesia, kebijakan pemerintah juga semakin menekankan digitalisasi pelayanan kesehatan. Hal ini tercermin melalui Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis, yang mewajibkan seluruh fasilitas pelayanan kesehatan menggunakan RME paling lambat akhir 2023. Peraturan ini menegaskan prinsip keamanan data yang meliputi kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Lebih lanjut, hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memperkuat kerangka hukum perlindungan data pasien di era digital.

Namun demikian, implementasi RME di Indonesia masih menghadapi sejumlah tantangan serius. Dari aspek teknis, berbagai penelitian menunjukkan bahwa sebagian rumah sakit baru memenuhi sekitar 40–49% dari standar keamanan ISO 27001. Kasus kebocoran data kesehatan—seperti insiden *ransomware* WannaCry pada 2017 yang melumpuhkan sistem di Rumah Sakit Dharmas dan Harapan Kita, serta kasus kebocoran data COVID-19 pada 2020—menunjukkan tingginya kerentanan sistem kesehatan terhadap serangan siber. Dari aspek non-teknis, kesadaran tenaga kesehatan dalam menjaga kerahasiaan data pasien juga masih relatif rendah, sehingga meningkatkan risiko terjadinya pelanggaran privasi.

Dengan demikian, isu keamanan data, privasi, dan kepastian hukum dalam implementasi RME menjadi sangat penting untuk dikaji lebih mendalam. Di satu sisi, RME menawarkan peluang besar dalam meningkatkan mutu layanan kesehatan; namun di sisi lain, lemahnya perlindungan terhadap data pasien dapat mengurangi kepercayaan masyarakat terhadap sistem kesehatan digital. Kajian literatur ini berupaya memberikan gambaran komprehensif mengenai kondisi terkini, tantangan, serta landasan hukum yang melingkupi penerapan RME di Indonesia.

Metode

Penelitian ini menggunakan pendekatan kualitatif dengan metode *literature review* yang berfokus pada analisis mendalam terhadap isu keamanan data, privasi, dan dasar hukum rekam medis elektronik (RME) di Indonesia. Data yang digunakan berasal dari sumber sekunder berupa artikel jurnal nasional dan internasional, buku, prosiding, serta regulasi resmi seperti Permenkes No. 24 Tahun 2022, UU

Perlindungan Data Pribadi, dan UU ITE. Literatur dikumpulkan melalui penelusuran basis data daring (Google Scholar, Crossref, Scopus, Portal Garuda) dengan kata kunci yang relevan. Proses analisis dilakukan secara deskriptif-kualitatif melalui tahapan reduksi data, kategorisasi temuan ke dalam tiga tema utama (aspek keamanan data, privasi dan kerahasiaan, serta dasar hukum), serta interpretasi untuk melihat hubungan antar-tema dan mengidentifikasi kesenjangan penelitian. Keabsahan data dijaga melalui triangulasi sumber, yaitu dengan membandingkan temuan empiris, teori akademik, dan regulasi yang berlaku, sehingga hasil kajian dapat dipertanggungjawabkan secara ilmiah.

Hasil

Tabel 1. Ringkasan Kajian Literatur terkait Keamanan Data, Privasi, dan Aspek Hukum dalam Implementasi Rekam Medis Elektronik di Indonesia

Judul Artikel	Penulis & Tahun	Hasil Penelitian	Strategi / Inovasi / Implikasi
Analisis Aspek Keamanan Informasi Data Pasien pada RME di Puskesmas Karangploso	Sofia, Ardianto, Muna & Sabran (2022)	Penelitian ini menganalisis penerapan sistem keamanan informasi pasien kesehatan pada RME di Puskesmas Karangploso, dengan latar belakang regulasi pemerintah yang mewajibkan penggunaan enkripsi, dan penerapan digitalisasi rekam medis. Penelitian menekankan pentingnya prinsip <i>confidentiality</i> , <i>integrity</i> , dan <i>availability</i> (CIA) dalam sistem kesehatan berbasis elektronik. Temuan menunjukkan adanya penerapan login berbasis <i>username-password</i> , pembatasan hak akses sesuai jabatan, serta backup data. Namun, kelemahan terlihat pada penggunaan akun bersama oleh beberapa petugas, yang membuat kontrol akses tidak efektif. Hal ini berpotensi menimbulkan kesalahan pencatatan, penyalahgunaan data, hingga pelanggaran privasi pasien. Secara umum, sistem keamanan dasar sudah diterapkan, tetapi kelemahan pada aspek perilaku pengguna menjadi tantangan utama. Hal ini menunjukkan bahwa aspek teknis perlu dibarengi dengan peningkatan literasi digital dan disiplin tenaga kesehatan agar privasi pasien terlindungi.	Perlunya edukasi tenaga kesehatan tentang penerapan <i>automatic log-off</i> , audit berkala agar aspek <i>confidentiality</i> , <i>integrity</i> , dan <i>availability</i> benar-benar diterapkan.
Kerahasiaan Medis dan Data Pasien dalam Catatan RME sesuai Permenkes No. 24/2022	Prisusanti & Afifah (2022)	Artikel ini menelaah isi Permenkes No. 24/2022 yang menggantikan PMK No. 269/2008, dengan fokus pada akses, kewajiban fasilitas kesehatan menjaga ketat kerahasiaan data pasien dalam RME. Regulasi ini dikeluarkan untuk menyesuaikan dengan perkembangan digitalisasi pelayanan kesehatan. Hasil analisis menunjukkan adanya pasal yang mewajibkan fasilitas kesehatan memberikan akses penuh data RME kepada Kementerian Kesehatan. Kebijakan ini menimbulkan dilema: di satu sisi mendukung integrasi data	Mekanisme izin pasien, transparansi pemerintah agar akses tidak disalahgunakan.

Judul Artikel	Penulis & Tahun	Hasil Penelitian	Strategi / Inovasi / Implikasi
Pelindungan Hak atas Rahasia Medis Pasien dalam Implementasi RME (RS Bhayangkara Semarang)	Rukayah & Khusniyah (2023)	melalui platform SATUSEHAT, tetapi di sisi lain melemahkan prinsip privasi pasien karena akses tidak lagi terbatas pada dokter atau institusi terkait. Dengan demikian, regulasi ini meskipun progresif, menyisakan celah yang dapat menimbulkan konflik hukum dan etika. Implikasi penelitian ini menekankan perlunya aturan turunan yang lebih detail untuk menyeimbangkan antara hak pasien atas kerahasiaan dengan kewajiban integrasi data nasional. Penelitian ini dilakukan di RS Rekomendasi: Bhayangkara Semarang untuk menilai peningkatan kapasitas bagaimana implementasi RME SDM, penyediaan sarana menjamin hak pasien atas kerahasiaan TI yang memadai, serta medis. Fokus penelitian adalah menilai sosialisasi UU PDP agar efektivitas kebijakan rumah sakit dalam perlindungan hukum lebih menjaga data medis pasien. Hasil efektif. penelitian menunjukkan bahwa perlindungan hak pasien dilakukan melalui kebijakan otorisasi akses terbatas, pengelolaan dokumen sesuai SOP, serta penyimpanan rekam medis yang aman. Namun, terdapat hambatan signifikan berupa keterbatasan infrastruktur TI dan kurangnya SDM yang memahami regulasi terkait perlindungan data. Secara keseluruhan, rumah sakit telah berupaya menjalankan kewajiban hukum, namun implementasi masih jauh dari sempurna. Hal ini memberi implikasi bahwa penguatan kapasitas SDM dan penyediaan sarana teknologi adalah kebutuhan mendesak agar hak pasien benar-benar terlindungi.	
Aspek Hukum Perlindungan Data Pasien dalam Implementasi RME di Era Digital	Rahmad & Budiman (2025)	Artikel ini menelaah kasus kebocoran data pasien di Indonesia (2019–2023) untuk melihat efektivitas regulasi, seperti UU PDP, UU ITE, dan Permenkes 24/2022. Tujuan utamanya adalah mengkaji sejauh mana regulasi yang ada mampu memberikan kepastian hukum bagi pasien. Penelitian menemukan 94 kasus kebocoran data, sebagian besar melibatkan penyalahgunaan sistem elektronik privat. Temuan ini menunjukkan lemahnya pengawasan dan minimnya kepatuhan fasilitas kesehatan terhadap standar keamanan digital. Banyak rumah sakit masih belum memiliki SOP yang sesuai regulasi. Dengan demikian, perlindungan hukum di Indonesia meskipun ada secara normatif, belum	Penegakan hukum yang tegas, harmonisasi antar-otoritas, dan pembentukan lembaga khusus untuk pengawasan keamanan data kesehatan.

Judul Artikel	Penulis & Tahun	Hasil Penelitian	Strategi / Inovasi / Implikasi
Analisis Dampak Keamanan Data Pasien pada Sistem RME di RS X	Omidah & Yunengsih (2024)	efektif secara implementatif. Penelitian ini menekankan bahwa regulasi harus diikuti dengan mekanisme sanksi yang jelas dan lembaga pengawas yang berfungsi secara aktif. Penelitian ini bertujuan menganalisis dampak keamanan data pasien dalam rutin, menerapkan rotasi penerapan RME di RS X. Studi dilakukan untuk melihat apakah sistem penguatan RME sudah memenuhi standar keamanan data yang berlaku. Temuan berbasis HIMSS <i>maturity index</i> menunjukkan sistem RME di RS X telah dilengkapi log aktivitas, VPN, dan tanda tangan elektronik bersertifikat. Namun, kelemahan besar ada pada tidak adanya audit internal dan belum adanya SOP rotasi password. Hal ini membuat sistem masih rentan terhadap serangan siber. Dengan demikian, meskipun sistem RME di RS X sudah memenuhi sebagian besar standar, keberlanjutan keamanan data sangat bergantung pada kebijakan internal. Implikasi penelitian ini menegaskan pentingnya audit berkelanjutan dan SOP yang konsisten.	Melakukan audit internal rutin, menerapkan rotasi password berkala, serta kebijakan keamanan informasi
Analisis Aspek Keamanan Data Pasien di RSI Sultan Agung	Indriyajati dkk. (2023)	Studi ini mengevaluasi kepatuhan sistem keamanan RME di RSI Sultan Agung terhadap standar ISO 27001. Fokus penelitian adalah mengukur sejauh mana aspek integritas dan autentikasi diterapkan. Hasil penelitian menemukan tingkat kepatuhan hanya 40–49%. Masalah utama terletak pada integritas data yang mudah diubah tanpa catatan, dan autentikasi pengguna yang hanya berbasis password tunggal. Implikasinya, meskipun ada komitmen untuk menerapkan standar internasional, implementasi masih jauh dari optimal. Penelitian ini memberi pesan penting bahwa tanpa investasi lebih pada keamanan TI, risiko kebocoran data tetap tinggi.	Rekomendasi: penerapan penuh ISO 27001, peningkatan autentikasi berlapis, dan integrasi sistem audit keamanan.
Implementasi SIMPUS Puskesmas (Integrasi Puskesmas)	Studi di Puskesmas Karangploso e- (2021)	Penelitian ini mengevaluasi penerapan Sistem Informasi Manajemen Puskesmas (SIMPUS) yang terintegrasi dengan e-Puskesmas. Fokus penelitian adalah keamanan dan konsistensi data. Hasil menunjukkan sistem login sudah diterapkan, tetapi integrasi antar unit layanan masih manual sehingga rawan inkonsistensi data. Keamanan data hanya mengandalkan <i>username-password</i> sederhana tanpa enkripsi. Implikasinya, meskipun SIMPUS	Perlu integrasi penuh SIMPUS dengan standar interoperabilitas, enkripsi data antar server, dan edukasi privasi bagi operator puskesmas.

Judul Artikel	Penulis & Tahun	Hasil Penelitian	Strategi / Inovasi / Implikasi
Aspek hukum perlindungan data pasien dalam implementasi Rekam Medis Elektronik (EMR) di era digital	Noor Rahmad, Eren Arif Budiman (2025)	mampu meningkatkan efisiensi, kelemahan keamanan masih menjadi celah yang perlu ditutup agar data pasien benar-benar terlindungi. Artikel ini menelaah berbagai kasus Harmonisasi UU PDP, UU kebocoran data di Indonesia, termasuk ITE, UU Rumah Sakit, dan data pasien COVID-19, untuk menguji Permenkes 24/2022; efektivitas UU PDP, UU ITE, dan penguatan sanksi regulasi kesehatan. Temuan administratif bagi menunjukkan bahwa meskipun pelanggaran kerangka hukum sudah ada, mekanisme implementasi belum optimal. Banyak lembaga kesehatan belum memahami kewajiban mereka, dan mekanisme perlindungan korban kebocoran belum jelas. Penelitian ini menekankan bahwa regulasi harus dilengkapi mekanisme pengawasan dan sanksi yang efektif agar perlindungan hukum bagi pasien benar-benar terwujud.	
Literature Review Keamanan Data Pasien pada RME di Indonesia (Narrative Review)	Ardianto, Sabran & Nurjanah (2024)	Artikel ini melakukan review terhadap Penerapan standar berbagai penelitian mengenai HIMSS; sistem monitoring keamanan data pasien di Indonesia. otomatis; Penerapan Fokus utamanya adalah menganalisis standar HIMSS, kekuatan dan kelemahan penerapan <i>continuous monitoring</i> , sistem RME. Hasil menunjukkan bahwa dan peningkatan sistem RME di banyak fasilitas kesadaran SDM tentang kesehatan sudah dilengkapi log keamanan data. aktivitas untuk mencatat akses pengguna, namun audit internal jarang dilakukan. Sistem lebih bersifat reaktif daripada proaktif. Implikasinya, keamanan data pasien masih rentan jika hanya mengandalkan log tanpa pengawasan aktif. Penelitian ini mendorong perlunya sistem deteksi dini ancaman dan peningkatan kesadaran keamanan di kalangan tenaga kesehatan.	

Pembahasan

Dalam upaya memahami dinamika implementasi Rekam Medis Elektronik (RME) di berbagai fasilitas pelayanan kesehatan, diperlukan analisis mendalam terhadap aspek-aspek fundamental yang memengaruhi keberhasilannya. Berdasarkan hasil telaah literatur dan berbagai penelitian empiris, terdapat tiga aspek utama yang menjadi fokus pembahasan, yaitu keamanan data, privasi dan kerahasiaan pasien, serta dasar hukum yang melandasi penerapannya. Ketiga aspek ini saling berkaitan dan membentuk satu kesatuan sistem yang menentukan sejauh mana RME dapat diimplementasikan secara efektif, aman, dan sesuai dengan ketentuan peraturan perundang-undangan

1. Aspek Keamanan Data

Dari hasil tinjauan, mayoritas jurnal menekankan bahwa keamanan data merupakan fondasi utama keberhasilan implementasi RME. Sistem yang digunakan di Puskesmas Karangploso sudah

memiliki fitur dasar seperti login individual, backup data, dan log aktivitas. Namun, adanya praktik berbagi akun dan lemahnya autentikasi menunjukkan bahwa penerapan keamanan belum sepenuhnya sesuai dengan standar(Sofia et al., 2022).

Kelemahan pada aspek keamanan juga terlihat dalam penelitian di RSI Sultan Agung, di mana tingkat kepatuhan terhadap ISO 27001 hanya berkisar 40–49%. Rendahnya kepatuhan ini menandakan bahwa fasilitas kesehatan belum siap menerapkan standar keamanan internasional(Sofia et al., 2022). Kondisi ini menunjukkan adanya kesenjangan antara kesiapan regulasi dan kapasitas teknis fasilitas kesehatan di lapangan.

Penelitian di RS X memberikan gambaran menarik. Meski sudah menggunakan VPN, tanda tangan elektronik, dan log aktivitas, kelemahan pada audit internal dan ketiadaan SOP rotasi password menjadikan sistem tetap rentan. Hal ini menegaskan bahwa penerapan teknologi saja tidak cukup jika tidak dibarengi dengan tata kelola internal yang baik dan konsistensi pengawasan.

Faktor manusia (human factor) juga menjadi penyebab signifikan lemahnya keamanan. Studi literatur menunjukkan bahwa kebiasaan tenaga kesehatan berbagi akun, kurang disiplin dalam logout, serta rendahnya literasi digital memperbesar risiko kebocoran data(Sofia et al., 2022). Hal ini sesuai dengan teori socio-technical system yang menekankan bahwa teknologi dan manusia harus berjalan seimbang dalam menjaga keamanan informasi.

Dengan demikian, penguatan keamanan RME tidak hanya bergantung pada perangkat keras dan perangkat lunak, tetapi juga harus didukung tata kelola internal, edukasi berkelanjutan, dan audit rutin. Penerapan multi-factor authentication, pengawasan independen, serta sosialisasi etika profesi merupakan langkah strategis agar keamanan data pasien dapat benar-benar terjamin.

2. Aspek Privasi dan Kerahasiaan

Privasi pasien muncul sebagai salah satu isu paling krusial. Artikel yang mengkaji Permenkes No. 24/2022 menemukan dilema ketika regulasi memberikan akses penuh data pasien kepada Kementerian Kesehatan. Kebijakan ini mendukung integrasi sistem nasional seperti SATUSEHAT, tetapi berisiko melemahkan privasi karena data pasien dapat diakses di luar kendali fasilitas kesehatan(Suhariyono et al., 2025).

Penelitian hukum Rahmad & Budiman (2025) menemukan adanya 94 kasus kebocoran data pasien dalam kurun 2019–2023, yang memperlihatkan lemahnya perlindungan privasi di Indonesia(Siregar & Haposan Sahala Raja Sinaga, 2025). Fakta ini mengindikasikan bahwa regulasi saja tidak cukup melindungi pasien tanpa adanya mekanisme pengawasan dan penegakan yang efektif.

Studi empiris di RS Bhayangkara Semarang justru menunjukkan hasil yang lebih positif. Rumah sakit berhasil menjaga kerahasiaan pasien melalui kebijakan otorisasi terbatas, penyimpanan aman, dan pemahaman staf terhadap prinsip kerahasiaan medis. Namun, penelitian ini juga menggarisbawahi kendala berupa keterbatasan SDM serta infrastruktur teknologi(Omidah & Yunengsih, 2025).

Sementara itu, penelitian lain menyoroti kelemahan perilaku tenaga kesehatan, misalnya berbagi password antar staf. Hal ini jelas melanggar prinsip privasi pasien dan membuka peluang

kebocoran data(Sofia et al., 2022). Dengan demikian, faktor kelalaian internal seringkali lebih berbahaya dibanding ancaman eksternal, karena dapat terjadi secara sistematis tanpa disadari.

Implikasi dari temuan-temuan ini adalah perlindungan privasi harus dilakukan melalui dua jalur: teknologi dan etika profesi. Teknologi seperti enkripsi, automatic log-off, dan log aktivitas penting untuk meminimalkan risiko, tetapi pembudayaan etika dan kedisiplinan tenaga kesehatan jauh lebih menentukan keberhasilan perlindungan privasi pasien.

3. Aspek Dasar Hukum

Indonesia sebenarnya telah memiliki kerangka hukum yang cukup lengkap terkait RME. Artikel tentang perlindungan hak atas rahasia medis menegaskan dasar hukum yang meliputi UUD 1945, UU PDP, UU ITE, hingga Permenkes No. 24/2022 sudah memadai(Rani & Widyaningrum, 2025). Regulasi ini memberi landasan normatif yang kuat untuk menjamin hak pasien atas kerahasiaan dan keamanan data medis.

Meski demikian, studi Anisah (2023) mengungkapkan bahwa banyak fasilitas kesehatan tidak memahami atau gagal menerapkan aturan hukum yang ada. Hal ini menimbulkan jurang besar antara teks regulasi dan praktik implementasi di lapangan(Suhariyono et al., 2025). Rendahnya pemahaman ini juga memperburuk lemahnya pengawasan pemerintah dalam memastikan kepatuhan fasilitas kesehatan.

Artikel Rahmad & Budiman (2025) memperkuat temuan ini dengan menyoroti bahwa regulasi sering gagal memberikan kepastian hukum bagi pasien korban kebocoran data(Siregar & Haposan Sahala Raja Sinaga, 2025). Banyak kasus kebocoran data tidak ditindaklanjuti dengan mekanisme hukum yang jelas, sehingga menimbulkan ketidakpastian dan kerugian bagi pasien.

Kondisi tersebut menunjukkan adanya regulatory gap, yaitu hukum tersedia tetapi tidak memiliki daya paksa yang cukup. Faktor pengawasan dan penegakan menjadi titik lemah yang membuat perlindungan hukum hanya bersifat formalitas. Akibatnya, pasien seringkali tidak mendapatkan pemulihan hak yang memadai setelah datanya bocor.

Untuk itu, efektivitas perlindungan hukum sangat bergantung pada konsistensi implementasi. Harmonisasi regulasi antar lembaga, kejelasan sanksi administratif, serta pengawasan aktif pemerintah harus diperkuat(Siregar & Haposan Sahala Raja Sinaga, 2025). Tanpa langkah konkret tersebut, perlindungan hukum hanya menjadi simbol normatif tanpa realisasi praktis di lapangan.

Simpulan dan saran

Implementasi Rekam Medis Elektronik (RME) di Indonesia menunjukkan kemajuan berarti, namun masih dihadapkan pada tantangan serius, terutama dalam aspek keamanan, privasi, dan dasar hukum. Dari sisi keamanan data, meskipun infrastruktur dasar seperti login individual, backup, dan log aktivitas telah diterapkan, kelemahan pada autentikasi, audit internal, serta faktor manusia menjadikan sistem tetap rentan. Hal ini menunjukkan perlunya penguatan budaya disiplin dan literasi digital di lingkungan tenaga kesehatan.

Dalam aspek privasi, regulasi seperti Permenkes No. 24/2022 menimbulkan dilema antara kebutuhan integrasi data dan perlindungan kerahasiaan pasien. Banyaknya kasus kebocoran data membuktikan bahwa teknologi tanpa pengawasan dan etika profesi tidak cukup untuk menjaga privasi.

Sementara itu, kerangka hukum yang ada sudah cukup komprehensif, namun lemahnya penegakan dan pengawasan menyebabkan perlindungan pasien belum optimal. Diperlukan harmonisasi regulasi, peningkatan kapasitas pengawasan, serta penegakan hukum yang konsisten agar perlindungan data pasien benar-benar terwujud.

Penguatan keamanan dan privasi RME sebaiknya dilakukan melalui pendekatan holistik yang mencakup pembaruan kebijakan keamanan, penerapan audit rutin, pelatihan literasi digital bagi tenaga kesehatan, serta sinergi antara pemerintah dan fasilitas pelayanan kesehatan dalam memastikan kepatuhan terhadap standar perlindungan data medis.

Daftar pustaka

- Omidah, & Yunengsih, Y. (2025). Analisis Dampak Keamanan Data Pasien Pada Sistem Rekam Medis Elektronik Di Rumah Sakit X. *Journal of Medical Record Student (JMeRS)*, 3, 83–88.
- Rani, D. M., & Widyaningrum, B. N. (2025). Evaluasi Keamanan Informasi Sistem Rekam Medis Elektronik di RSI Sultan Agung. *Jurnal Manajemen Informasi Kesehatan (Health Information Management)*, 10(1), 52–62. <https://ojs.stikessaptabakti.ac.id/jmis/article/view/636>
- Siregar, R. A., & Haposan Sahala Raja Sinaga. (2025). Aspek Hukum Perlindungan Data Pasien Dalam Penyelenggaraan Rekam Medis Elektronik Di Indonesia. *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat*, 11(1), 106–116. <https://doi.org/10.55809/tora.v11i1.433>
- Sofia, S., Ardianto, E. T., Muna, N., & Sabran, S. (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>
- Suhariyono, U. S., Rusdian Ikawati, F., & Afifah, N. (2025). Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso. *Jurnal Manajemen Informasi Kesehatan Indonesia*, 13(1), 2337–2585.