SENTRI: Jurnal Riset Ilmiah
https://ejournal.nusantaraglobal.ac.id/index.php/sentri
Email: sentri@nusantaraglobal.ac.id
DOI: https://doi.org/10.55681/sentri.v5i2.5603

Vol. 5, No. 2, February 2026
e-ISSN: 2963-1130
pp. 1417-1436

Analisis Yuridis Upaya Pencegahan dan Risiko Hukum terhadap Kebocoran Data Rekam Medis Elektronik Pasien di RSUD Serpong Utara

Alya Puspita Juliasari[1*], Idris Wasahua[1]
[1] Universitas Esa Unggul, Fakultas Hukum, Jurusan Ilmu Hukum, Jl. Arjuna Utara No.9, Duri Kepa, Kebon Jeruk, Jakarta Barat 11510.

*Corresponding Author's e-mail: alyapuspita714@student.esaunggul.ac.id

Article History:
Received: January 5, 2026
Revised: January 27, 2026
Accepted: February 21, 2026

Keywords:
Data Protection,
EMR,
Legal Compliance,
Patient Data Leakage Risk

Abstract: *The advancement of digitalization in healthcare services requires hospitals to implement Electronic Medical Records (EMRs) supported by secure, accurate, and integrated data management. This study aims to analyze the compliance of data breach prevention measures for patient EMRs at RSUD Serpong Utara with national legal provisions and to assess the potential legal risks arising from data breaches. The research employs a normative–empirical juridical approach, with data collected through in-depth interviews with the Medical Records Coordinator, EMR implementing officers, Head of the IT Team, Public Relations officers, and the Chair of the Quality Committee, as well as analysis of internal documents and relevant laws and regulations. The findings indicate that RSUD Serpong Utara has implemented access control mechanisms, individual user accounts, hierarchical supervision, and data storage on external servers to prevent data breaches. However, EMR implementation remains hybrid in several units, the CPPT audit trail has not been effectively implemented, and there is no appointed Data Protection Officer or internal legal unit. The enactment of Law No. 27 of 2022 on Personal Data Protection (UU PDP) establishes a more stringent regulatory standard compared to previous regulations, demanding comprehensive compliance from healthcare institutions in protecting patient data. The potential legal risks include administrative sanctions, civil liability claims, and criminal liability. Based on normative juridical analysis of the applicable laws and regulations and empirical findings regarding EMR management practices at RSUD Serpong Utara, this study concludes that strengthening EMR governance through the completion of digital transition, the appointment of a Data Protection Officer, the establishment of an internal legal unit, and the effective implementation of incident audits and audit trails is necessary to enhance legal compliance and reduce the risk of patient data breaches.*

Copyright © 2026, The Author(s).
This is an open access article under the CC–BY-SA license

How to cite: Juliasari, A. P., & Wasahua, I. (2026). Analisis Yuridis Upaya Pencegahan dan Risiko Hukum terhadap Kebocoran Data Rekam Medis Elektronik Pasien di RSUD Serpong Utara. SENTRI: Jurnal Riset Ilmiah, 5(2), 1417–1436. https://doi.org/10.55681/sentri.v5i2.5603

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan yang cukup signifikan dalam sistem pelayanan publik, khususnya di sektor kesehatan, yang menuntut peningkatan efisiensi, akurasi, dan keamanan informasi pasien (Agustina Tifanny, 2025). Salah satu inovasi utama yang kini banyak diterapkan oleh rumah sakit di Indonesia adalah Rekam Medis Elektronik (RME), sebuah sistem yang memungkinkan pengelolaan data kesehatan pasien secara terstruktur, menyeluruh, dan terintegrasi antarunit layanan (Izza & Lailiyah, 2024). Sistem rekam medis digital juga mencakup catatan medis, laporan

laboratorium, rekam prosedur perawatan, resep obat, hingga dokumentasi lain yang berkaitan dengan proses pelayanan medis (Wijayanta Setya, 2024). Sistem ini dirancang untuk mempercepat akses informasi bagi tenaga medis serta meningkatkan mutu dan efektivitas pelayanan kesehatan (Neng Sari Rubiyanti, 2023).

Di sisi lain, penerapan sistem digital ini juga menghadirkan tantangan hukum dan etika, khususnya terkait kerahasiaan informasi pasien, perlindungan hak privasi, dan potensi kebocoran data. Apabila tidak dikelola secara tepat, masalah tersebut dapat menimbulkan konsekuensi hukum yang serius bagi institusi kesehatan (Nadiroh & Wiraguna, 2025). Urgensi perlindungan data kesehatan pasien semakin mengemuka seiring dengan terjadinya sejumlah kasus kebocoran data yang melibatkan institusi kesehatan di Indonesia dalam beberapa tahun terakhir. Insiden kebocoran data BPJS Kesehatan pada Mei 2021 yang mengekspos informasi pribadi lebih dari 279 juta penduduk Indonesia, termasuk Nomor Induk Kependudukan (NIK), alamat, nomor telepon, hingga riwayat kesehatan, menjadi salah satu kasus kebocoran data terbesar di Indonesia dan menimbulkan keresahan publik yang masif. Selain itu, pada tahun 2020, terjadi kebocoran data pasien COVID-19 yang meliputi identitas, hasil tes laboratorium, dan riwayat perjalanan yang diperjualbelikan secara ilegal di forum-forum daring. Kasus lain yang juga menarik perhatian adalah kebocoran data pasien dari beberapa rumah sakit swasta yang mengakibatkan penyalahgunaan informasi untuk penipuan asuransi dan eksploitasi komersial tanpa persetujuan pasien. Rangkaian insiden tersebut tidak hanya mencederai kepercayaan publik terhadap sistem kesehatan digital, tetapi juga menggarisbawahi kerentanan infrastruktur keamanan data di sektor kesehatan Indonesia serta lemahnya mekanisme pengawasan dan penegakan hukum terhadap pelindungan data pribadi pasien.

Kondisi ini menimbulkan celah pengaturan yang dapat meningkatkan potensi kebocoran data pasien serta menimbulkan risiko pertanggungjawaban hukum bagi rumah sakit, baik pidana, perdata, maupun administratif (Tovino A, 2022). Sebagai konsekuensinya, dampak tidak hanya dirasakan oleh pasien sebagai subjek data, tetapi juga memengaruhi tanggung jawab hukum rumah sakit sebagai pengendali data (Purnomo & Mashuri, 2025). Pada tingkat operasional RSUD Serpong Utara, berbagai tantangan terkait kapasitas sumber daya manusia, kebijakan internal, dan pemahaman terhadap regulasi semakin menegaskan perlunya penguatan tata kelola rekam medis elektronik dalam penerapannya. Peningkatan kasus kebocoran data kesehatan dalam lima tahun terakhir, termasuk terekspos nya data identitas, riwayat layanan, dan informasi medis pada insiden BPJS Kesehatan 2021 serta bocornya data pasien COVID-19 2020, menunjukkan kelemahan signifikan dalam sistem perlindungan data (Tatang Guritno, 2022).

Berdasarkan paparan latar belakang tersebut, dapat dirumuskan permasalahan yang menjadi fokus kajian sebagai berikut:

1. Apakah upaya pencegahan kebocoran data rekam medis elektronik pasien di RSUD Serpong Utara telah sesuai dengan ketentuan hukum yang mengatur kerahasiaan informasi kesehatan dan perlindungan hak privasi pasien?
2. Bagaimana bentuk risiko hukum yang dapat timbul jika terjadi kebocoran data rekam medis elektronik pasien di RSUD Serpong Utara?

LANDASAN TEORI

2.1 Rekam Medis Elektronik (RME)

Rekam Medis Elektronik (RME) atau Electronic Medical Records (EMR) merupakan sistem pengelolaan data kesehatan pasien secara terstruktur, menyeluruh, dan terintegrasi antarunit layanan dalam format digital [1]. Sistem ini mencakup catatan medis, laporan laboratorium, rekam prosedur perawatan, resep obat, hingga dokumentasi lain yang berkaitan dengan proses pelayanan medis [2]. RME dirancang untuk mempercepat akses informasi bagi tenaga medis serta meningkatkan mutu dan efektivitas pelayanan kesehatan [3].

Implementasi RME di Indonesia diatur dalam Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis [4], yang mengatur standar penyelenggaraan rekam medis baik dalam bentuk elektronik maupun manual. Permenkes ini menetapkan bahwa rekam medis elektronik harus memenuhi prinsip keamanan, kerahasiaan, integritas, ketersediaan, dan ketertelusuran data [4][5]. Penerapan RME di rumah sakit Indonesia menghadapi berbagai tantangan, baik dari aspek teknis maupun non-teknis. Tantangan teknis meliputi integrasi data kesehatan dari berbagai sistem yang berbeda dalam satu platform terpadu [6], sedangkan tantangan non-teknis mencakup kesiapan sumber daya manusia, infrastruktur teknologi informasi, dan pemahaman terhadap regulasi yang berlaku [7][8].

2.2 Perlindungan Data Pribadi Pasien

Data pribadi pasien dalam rekam medis termasuk dalam kategori data pribadi yang bersifat spesifik dan sensitif karena menyangkut informasi kesehatan yang dilindungi kerahasiaannya [9]. Perlindungan data pribadi pasien diatur dalam beberapa regulasi, antara lain:

2.2.1 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

UU Pelindungan Data Pribadi (UU PDP) [10] memberikan landasan hukum yang komprehensif dalam perlindungan data pribadi di Indonesia. Undang-undang ini mengatur hak-hak subjek data pribadi, kewajiban pengendali dan prosesor data pribadi, serta sanksi bagi pelanggarnya. UU PDP menetapkan prinsip-prinsip pemrosesan data pribadi yang meliputi: (a) keabsahan dan keadilan; (b) pembatasan tujuan; (c) keakuratan; (d) pertanggungjawaban; (e) penyimpanan terbatas; dan (f) integritas dan kerahasiaan.

Dalam konteks data kesehatan, UU PDP mengklasifikasikan data kesehatan sebagai data pribadi yang bersifat spesifik yang memerlukan perlindungan khusus [10]. Pengendali data pribadi, dalam hal ini rumah sakit, wajib menunjuk Pejabat Pelindung Data Pribadi (Data Protection Officer/DPO) yang bertugas mengawasi kepatuhan terhadap peraturan pelindungan data pribadi [11].

2.2.2 Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan

UU Kesehatan [12] mengatur secara khusus tentang kerahasiaan rekam medis dan kewajiban tenaga kesehatan serta fasilitas pelayanan kesehatan untuk menjaga kerahasiaan data pasien. Pasal 343 UU Kesehatan menegaskan bahwa rekam medis harus

dijaga kerahasiaannya dan hanya dapat dibuka untuk kepentingan kesehatan pasien, penegakan hukum, permintaan pasien sendiri, atau atas perintah pengadilan.

2.2.3 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

UU ITE [13] mengatur aspek keamanan sistem elektronik dan perlindungan data pribadi dalam sistem elektronik. Pasal 26 UU ITE mewajibkan penyelenggara sistem elektronik untuk melindungi data pribadi pengguna dari akses dan penggunaan yang tidak sah. Pelanggaran terhadap ketentuan ini dapat dikenakan sanksi pidana sebagaimana diatur dalam Pasal 48 jo. Pasal 26 UU ITE.

2.2.4 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

PP 71/2019 [14] mengatur lebih lanjut mengenai penyelenggaraan sistem elektronik yang aman, andal, dan bertanggung jawab. Peraturan ini mewajibkan penyelenggara sistem elektronik untuk menerapkan manajemen risiko, audit sistem elektronik secara berkala, serta menyediakan audit trail untuk menelusuri jejak aktivitas dalam sistem.

2.3 Keamanan dan Kerahasiaan Data Rekam Medis Elektronik

Keamanan data RME mencakup tiga aspek utama, yaitu: (1) kerahasiaan (confidentiality) yang memastikan data hanya dapat diakses oleh pihak yang berwenang; (2) integritas (integrity) yang menjamin data tidak diubah atau dimanipulasi tanpa otorisasi; dan (3) ketersediaan (availability) yang memastikan data dapat diakses ketika dibutuhkan [15].

Implementasi keamanan data RME memerlukan penerapan berbagai mekanisme teknis dan administratif, antara lain [16][17]:

1. Kontrol Akses (Access Control): Pembatasan akses terhadap data berdasarkan peran dan kewenangan pengguna melalui sistem autentikasi dan autorisasi yang kuat.
2. Enkripsi Data: Pengamanan data baik saat penyimpanan (data at rest) maupun saat transmisi (data in transit) melalui teknologi enkripsi.
3. Audit Trail: Pencatatan seluruh aktivitas akses dan perubahan data untuk memastikan ketertelusuran dan akuntabilitas.
4. Backup dan Recovery: Sistem pencadangan data secara berkala dan prosedur pemulihan data untuk mengantisipasi kehilangan data.
5. Pemisahan Tugas (Segregation of Duties): Pemisahan peran dan tanggung jawab untuk mencegah penyalahgunaan kewenangan.

2.4 Kebocoran Data dan Risiko Hukum

Kebocoran data (data breach) didefinisikan sebagai insiden keamanan yang mengakibatkan akses, pengambilan, pengungkapan, pengubahan, atau penghancuran data pribadi secara tidak sah [18]. Dalam konteks data kesehatan, kebocoran data dapat terjadi melalui berbagai cara, antara lain: serangan siber (hacking), human error, penyalahgunaan kewenangan oleh pihak internal, atau kelemahan sistem keamanan [19].

Beberapa kasus kebocoran data kesehatan yang terjadi di Indonesia menunjukkan kerentanan sistem perlindungan data di sektor kesehatan. Insiden kebocoran data BPJS Kesehatan pada tahun 2021 yang mengekspos informasi pribadi lebih dari 279 juta penduduk Indonesia menjadi salah satu kasus terbesar dan menimbulkan keresahan publik yang masif [20]. Kasus lain yang juga mencuat adalah kebocoran data pasien COVID-19 pada tahun 2020 yang meliputi identitas, hasil tes laboratorium, dan riwayat perjalanan [21].

2.4.1 Risiko Hukum Administratif

Berdasarkan UU PDP [10], pengendali data pribadi yang melanggar ketentuan perlindungan data dapat dikenakan sanksi administratif berupa:a. Peringatan tertulis; b. Penghentian sementara kegiatan pemrosesan data pribadi; c. Penghapusan atau pemusnahan data pribadi; d. Denda administratif paling banyak 2% (dua persen) dari pendapatan tahunan atau penerimaan tahunan.

Selain itu, Permenkes 24/2022 [4] juga mengatur sanksi administratif bagi fasilitas pelayanan kesehatan yang tidak menjaga kerahasiaan rekam medis, yang dapat berupa teguran lisan, teguran tertulis, hingga pencabutan izin operasional.

2.4.2 Risiko Hukum Perdata

Kebocoran data rekam medis dapat menimbulkan tuntutan ganti rugi berdasarkan prinsip perbuatan melawan hukum (onrechtmatige daad) sebagaimana diatur dalam Pasal 1365 KUH Perdata [22]. Pasien sebagai subjek data yang dirugikan akibat kebocoran data dapat menuntut kompensasi materiil maupun immateriil kepada rumah sakit sebagai pengendali data.

UU PDP [10] juga memberikan hak kepada subjek data pribadi untuk mengajukan gugatan ganti rugi atas kerugian yang diderita akibat pelanggaran pelindungan data pribadi. Beban pembuktian dalam gugatan ini dapat dialihkan kepada pengendali data pribadi apabila terdapat indikasi kelalaian dalam melindungi data pribadi.

2.4.3 Risiko Hukum Pidana

Tindak pidana terkait kebocoran data rekam medis dapat dijerat dengan berbagai ketentuan pidana, antara lain [23]:

1. UU ITE Pasal 32: Mengatur larangan mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun dengan ancaman pidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp800.000.000,00.
2. UU PDP Pasal 67: Mengatur pidana terhadap setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat merugikan subjek data pribadi, dengan ancaman pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5.000.000.000,00.
3. UU Kesehatan Pasal 546: Mengatur pidana bagi tenaga kesehatan yang dengan sengaja membuka rahasia kedokteran, dengan ancaman pidana penjara paling lama 1 tahun atau denda paling banyak Rp100.000.000,00.

2.5 Tata Kelola Data dan Kepatuhan Hukum Rumah Sakit

Tata kelola data (data governance) di rumah sakit merupakan kerangka kerja yang mengatur pengelolaan data secara efektif, efisien, dan sesuai dengan regulasi yang berlaku [24]. Tata kelola yang baik mencakup penetapan kebijakan, prosedur, struktur organisasi, serta mekanisme pengawasan dan evaluasi terhadap pengelolaan data [25].

Untuk memastikan kepatuhan hukum terhadap regulasi perlindungan data pribadi, rumah sakit perlu menerapkan beberapa langkah strategis [26]:

1. Penunjukan Data Protection Officer (DPO): Sesuai amanat UU PDP, rumah sakit wajib menunjuk DPO yang bertugas mengawasi implementasi kebijakan pelindungan data pribadi.
2. Penyusunan Kebijakan Internal: Penetapan Standard Operating Procedure (SOP) yang jelas terkait pengelolaan, akses, dan keamanan data rekam medis elektronik.
3. Pelatihan dan Edukasi SDM: Peningkatan kapasitas dan kesadaran tenaga kesehatan serta staf IT mengenai pentingnya perlindungan data pribadi pasien.
4. Audit dan Monitoring: Pelaksanaan audit berkala terhadap sistem keamanan data dan kepatuhan terhadap regulasi.
5. Incident Response Plan: Penyusunan prosedur penanganan insiden kebocoran data yang cepat dan efektif.
6. Pembentukan Unit Hukum Internal: Keberadaan unit hukum internal dapat membantu rumah sakit dalam mengidentifikasi risiko hukum, memberikan legal advice, serta menangani permasalahan hukum yang muncul.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif-empiris, yang memadukan analisis terhadap peraturan perundang-undangan dengan data empiris yang diperoleh dari lapangan [26]. Pendekatan normatif dilakukan melalui studi kepustakaan terhadap regulasi terkait perlindungan data pribadi dan rekam medis elektronik, meliputi UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [10], UU Nomor 17 Tahun 2023 tentang Kesehatan [12], UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik [13], PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik [14], serta Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis [4]. Sementara itu, pendekatan empiris dilakukan melalui penelitian lapangan di RSUD Serpong Utara untuk memperoleh data primer mengenai praktik pengelolaan RME dan upaya pencegahan kebocoran data pasien.

Subjek penelitian ditetapkan melalui teknik purposive sampling, yaitu pemilihan informan berdasarkan tugas, kewenangan, dan keterlibatan langsung mereka dalam pengelolaan RME [26]. Pemilihan informan dilakukan secara strategis dengan mempertimbangkan representasi dari berbagai aspek pengelolaan RME di RSUD Serpong Utara. Informan yang dipilih terdiri atas:

1. Koordinator Rekam Medis: dipilih sebagai informan kunci karena memiliki tanggung jawab langsung dalam pengelolaan, pengawasan, dan penetapan kebijakan terkait rekam medis elektronik sesuai dengan Permenkes 24/2022 [4], serta memahami aspek teknis dan regulasi yang berlaku dalam pelaksanaan RME di rumah sakit [3][7].

2. Petugas Pelaksana Rekam Medis: dipilih untuk memberikan perspektif operasional mengenai praktik sehari-hari dalam penggunaan sistem RME, termasuk mekanisme akses data, prosedur keamanan, dan kendala yang dihadapi di tingkat implementasi [8].
3. Kepala Tim IT (Information Technology): dipilih karena memiliki kompetensi teknis dalam pengelolaan infrastruktur teknologi informasi, keamanan sistem, server penyimpanan data, serta bertanggung jawab atas aspek teknis keamanan data RME [1][6].
4. Humas Rumah Sakit: dipilih untuk memperoleh informasi mengenai kebijakan komunikasi publik, penanganan keluhan terkait data pasien, serta prosedur pelaporan insiden yang melibatkan aspek reputasi institusi.
5. Ketua Komite Mutu: dipilih karena memiliki peran dalam pengawasan mutu pelayanan, audit internal, dan evaluasi kepatuhan terhadap standar pelayanan serta regulasi yang berlaku di rumah sakit [5].

Pemilihan kelima informan tersebut dianggap representatif karena mencakup seluruh elemen kunci dalam ekosistem pengelolaan RME, mulai dari aspek kebijakan dan regulasi (Koordinator Rekam Medis), implementasi teknis dan keamanan sistem (Kepala Tim IT), pelaksanaan operasional (Petugas Pelaksana), komunikasi dan manajemen risiko reputasi (Humas), hingga pengawasan mutu dan kepatuhan (Ketua Komite Mutu). Kombinasi informan dari berbagai lini ini memungkinkan peneliti memperoleh gambaran komprehensif mengenai upaya pencegahan kebocoran data dan risiko hukum yang dihadapi RSUD Serpong Utara.

Pengumpulan data lapangan dilakukan pada bulan Desember 2024, dengan wawancara mendalam (in-depth interview) dilaksanakan pada tanggal 4 Desember 2024. Wawancara dirancang untuk menggali informasi mengenai upaya RSUD Serpong Utara dalam mencegah kebocoran data pasien, mekanisme kontrol akses, prosedur audit trail, kebijakan perlindungan data, serta menilai kesesuaiannya dengan ketentuan hukum yang mengatur pelindungan data dan kerahasiaan rekam medis [9][11].

Selain wawancara, penelitian ini juga menggunakan teknik pengumpulan data melalui studi dokumentasi terhadap dokumen internal rumah sakit, meliputi Standar Operasional Prosedur (SOP) pengelolaan RME, kebijakan keamanan data, struktur organisasi pengelola data, log sistem akses, dan laporan audit internal yang relevan dengan pengelolaan data pasien [17].

Untuk menjamin validitas dan reliabilitas data, penelitian ini menerapkan teknik triangulasi data melalui tiga pendekatan [26]:

1. Triangulasi Sumber: membandingkan dan mengecek informasi yang diperoleh dari berbagai informan yang memiliki perspektif berbeda (Koordinator Rekam Medis, Petugas Pelaksana, Kepala Tim IT, Humas, dan Ketua Komite Mutu) untuk memastikan konsistensi dan akurasi data.
2. Triangulasi Metode: membandingkan data yang diperoleh melalui wawancara mendalam dengan data dari dokumen internal rumah sakit, seperti SOP, kebijakan keamanan data, dan log sistem, sehingga informasi yang diperoleh dapat diverifikasi secara silang.
3. Triangulasi Teori: menganalisis temuan empiris dengan kerangka hukum normatif yang berlaku, yaitu membandingkan praktik pengelolaan RME di RSUD Serpong

Utara dengan ketentuan dalam UU PDP [10], UU Kesehatan [12], UU ITE [13], PP 71/2019 [14], dan Permenkes 24/2022 [4], untuk menilai tingkat kepatuhan dan mengidentifikasi potensi risiko hukum.

Analisis data dilakukan secara deskriptif-kualitatif dengan memadukan penelaahan normatif terhadap regulasi dan temuan empiris di lapangan [26]. Proses analisis dilakukan melalui tahapan: (1) reduksi data, yaitu pemilihan dan penyederhanaan data mentah dari wawancara dan dokumen; (2) penyajian data, yaitu pengorganisasian data dalam bentuk narasi dan tabel untuk memudahkan interpretasi; (3) penarikan kesimpulan, yaitu mengidentifikasi pola, tema, dan hubungan antara temuan empiris dengan kerangka hukum normatif; serta (4) verifikasi, yaitu pengecekan kembali terhadap validitas kesimpulan melalui triangulasi data [26].

Pendekatan ini dipilih untuk memastikan bahwa penilaian atas kepatuhan dan tata kelola keamanan data tidak hanya didasarkan pada kerangka hukum yang berlaku, tetapi juga mencerminkan kondisi nyata di rumah sakit [16][18][19]. Dengan demikian, penelitian ini menghasilkan gambaran yang lebih komprehensif dan dapat dipertanggungjawabkan secara ilmiah mengenai upaya pencegahan kebocoran data RME dan risiko hukum yang dihadapi RSUD Serpong Utara dalam konteks implementasi UU Pelindungan Data Pribadi dan regulasi terkait lainnya.

HASIL DAN PEMBAHASAN

Analisis Kepatuhan Upaya Pencegahan Kebocoran Data Rekam Medis Elektronik di RSUD Serpong Utara

Kepatuhan terhadap upaya pencegahan kebocoran data rekam medis elektronik dianalisis melalui pengujian kesesuaian antara praktik pengelolaan rekam medis di RSUD Serpong Utara dan ketentuan peraturan perundang-undangan yang mengatur kerahasiaan informasi kesehatan serta perlindungan data pribadi pasien. Pengaturan hukum tidak hanya mengatur hak pasien memperoleh pelayanan dan perlindungan informasi, tetapi juga menetapkan kewajiban rumah sakit untuk menyimpan data pasien dengan aman [16].

Dalam penyelenggaraan rekam medis elektronik terdapat dua jenis peraturan yang menjadi dasar hukum dan pedoman operasional, yaitu peraturan umum dan peraturan khusus. Peraturan umum berfungsi sebagai payung hukum yang mengatur prinsip dasar pengelolaan sistem elektronik, termasuk keamanan dan integritas data. Peraturan khusus mengatur ketentuan teknis terkait penyelenggaraan rekam medis elektronik, hak dan kewajiban pasien, tenaga medis, serta fasilitas kesehatan, terutama dalam hal perlindungan data dan privasi pasien [25].

Di bawah ini adalah pengaturan hukum yang mengatur tentang penyelenggaraan Rekam Medis Elektronik (RME), tata kelola sistem informasi kesehatan, serta perlindungan data pribadi pasien, yang menjadi dasar normatif bagi pelaksanaan rekam medis di berbagai fasilitas pelayanan kesehatan, antara lain sebagai berikut:

1. **Peraturan hukum yang bersifat umum** meliputi UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang menegaskan setiap informasi identitas individu, termasuk rekam medis elektronik pasien, merupakan data pribadi yang wajib dilindungi [23]. Setiap pemrosesan data harus dilakukan secara sah, terbatas, jujur, akurat, dan aman, serta memerlukan penunjukan pejabat perlindungan data

pribadi dengan kompetensi hukum sesuai Pasal 1 ayat 1, Pasal 4 ayat 2, Pasal 16 ayat 1–2 dan Pasal 53 [10]. Perlindungan ini diperkuat UU Nomor 11 Tahun 2008 Jo UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang melarang penyalahgunaan informasi elektronik dan mewajibkan pencegahan serta pemutusan akses bila terjadi pelanggaran hukum sesuai Pasal 27A dan Pasal 40 ayat 2 [13]. Selain itu, PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menekankan kewajiban penyelenggara sistem untuk menjaga keamanan, melindungi data dari kerugian, dan menghapus informasi tidak relevan atas permintaan subjek data sesuai Pasal 5 ayat 1, Pasal 15 ayat 1 dan Pasal 24 ayat 1 [14].

2. **Peraturan hukum yang bersifat khusus** meliputi Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik yang mewajibkan fasilitas kesehatan menyelenggarakan rekam medis elektronik secara terintegrasi dan aman. Regulasi ini juga menegaskan bahwa isi rekam medis merupakan informasi mengenai kondisi pasien yang wajib dijaga kerahasiaannya, serta pasien memiliki hak untuk mengakses dan memperoleh salinan atas informasi tersebut [24]. Akses terhadap tenaga kesehatan dan Kementerian Kesehatan diatur untuk menjamin kerahasiaan, keamanan, integritas, dan ketersediaan data sesuai Pasal 1 ayat 1–2, Pasal 3, Pasal 6 sampai 8, Pasal 21 dan Pasal 26 sampai 31 [4]. Selain itu, UU Nomor 17 Tahun 2023 tentang Kesehatan menegaskan hak pasien atas kerahasiaan informasi kesehatan dan akses terhadap rekam medis, serta menekankan tanggung jawab kolektif tenaga medis, pimpinan fasilitas pelayanan kesehatan, dan Kementerian Kesehatan dalam pengelolaan data sesuai Pasal 4 ayat 1 huruf i, Pasal 276, Pasal 296 ayat 5, Pasal 297 dan Pasal 298 [12].

Pemberlakuan UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menandai era baru dalam perlindungan data kesehatan di Indonesia dengan menetapkan standar yang jauh lebih ketat dan komprehensif dibandingkan regulasi sebelumnya [10]. Berbeda dengan UU ITE yang hanya mengatur perlindungan data secara umum dan Permenkes yang fokus pada aspek teknis rekam medis, UU PDP secara khusus mengatur prinsip-prinsip pemrosesan data pribadi, kewajiban penunjukan Data Protection Officer (DPO), mekanisme persetujuan subjek data, hak subjek data untuk mengakses dan menghapus data, serta sanksi yang lebih tegas baik administratif maupun pidana [11]. Regulasi ini juga mengklasifikasikan data kesehatan sebagai data pribadi spesifik yang memerlukan perlindungan paling tinggi, sehingga rumah sakit tidak lagi hanya bertanggung jawab atas kerahasiaan informasi medis sebagaimana diatur dalam regulasi sebelumnya, tetapi juga wajib memenuhi seluruh prinsip pemrosesan data yang meliputi keabsahan, pembatasan tujuan, keakuratan, akuntabilitas, penyimpanan terbatas, integritas, dan kerahasiaan [10][11]. Konsekuensinya, RSUD Serpong Utara sebagai pengendali data pribadi dituntut untuk melakukan transformasi tata kelola data secara menyeluruh, termasuk penguatan infrastruktur keamanan, pembentukan mekanisme audit yang efektif, dan peningkatan kapasitas SDM dalam memahami kewajiban hukum yang lebih kompleks dibandingkan sebelum UU PDP diberlakukan.

Ketentuan-ketentuan tersebut menjadi landasan normatif untuk menilai kepatuhan RSUD Serpong Utara dalam pengelolaan rekam medis elektronik, efektivitas upaya pencegahan kebocoran data, serta potensi risiko hukum apabila kewajiban perlindungan data tidak dijalankan dengan baik.

RSUD Serpong Utara mulai mengimplementasikan Rekam Medis Elektronik (RME) pada Agustus 2023. Namun, hingga saat ini, digitalisasi rekam medis belum dapat diterapkan secara penuh di seluruh unit pelayanan. Implementasi rekam medis digital baru berjalan secara menyeluruh pada unit poliklinik, sementara unit rawat inap dan Instalasi Gawat Darurat (IGD) masih menggunakan sistem hybrid yang mengombinasikan pencatatan manual dan digital.

Pembagian tugas dalam pengelolaan Rekam Medis Elektronik (RME) di RSUD Serpong Utara dilakukan berdasarkan struktur unit kerja. Unit Rekam Medis memiliki tanggung jawab utama terhadap pengolahan data pasien. Secara operasional, alur pemrosesan data dimulai sejak pasien melakukan pendaftaran pada layanan Instalasi Gawat Darurat (IGD) atau poliklinik. Data tersebut kemudian terintegrasi dengan berbagai layanan penunjang, seperti rawat inap, laboratorium, dan farmasi. Mekanisme ini menunjukkan bahwa meskipun sistem telah mengadopsi digitalisasi melalui RME, koordinasi antarsatuan kerja tetap menjadi komponen penting untuk memastikan kelancaran pemrosesan informasi pasien [8].

Mekanisme pengelolaan RME di RSUD Serpong Utara masih dalam tahap pengembangan seiring transisi dari sistem manual ke digital. Penanganan kesalahan input maupun dugaan penyimpangan akses dilakukan melalui pelaporan langsung ke tim IT sebagai bagian dari alur kerja internal. Ketiadaan prosedur tertulis khusus disebabkan belum adanya temuan penyimpangan, sehingga rumah sakit sementara mengandalkan mekanisme internal untuk menjaga konsistensi dan akurasi data.

RSUD Serpong Utara hingga kini belum memiliki unit legal tersendiri, sehingga penanganan isu yang berhubungan dengan aspek hukum masih dilakukan melalui koordinasi antarunit, seperti pimpinan unit terkait dan bagian IT, sesuai pembagian tugas yang berlaku di lingkungan rumah sakit.

Dalam hal keamanan data, setiap indikasi aktivitas sistem yang dianggap tidak normal segera dilaporkan kepada Dinas Komunikasi dan Informatika (Kominfo) selaku pengelola server dan database untuk dilakukan pemeriksaan serta tindak lanjut sesuai kewenangan. Prosedur pelaporan terhadap potensi gangguan keamanan maupun dugaan penyimpangan akses juga disampaikan kepada Kominfo sebagai bagian dari mekanisme pengawasan bersama.

Namun hingga saat ini, tidak pernah ditemukan adanya insiden akses data yang tidak sah, dan upaya penguatan terhadap perlindungan data pasien terus dilakukan sejalan dengan perkembangan digitalisasi serta penyesuaian terhadap regulasi nasional yang mengatur penyelenggaraan sistem elektronik, keamanan data, perlindungan privasi, dan tata kelola informasi di sektor kesehatan.

Pelindungan data pasien dalam Rekam Medis Elektronik (RME) di RSUD Serpong Utara dilaksanakan dengan menekankan prinsip kerahasiaan, integritas, dan keamanan informasi, serta berorientasi pada kepatuhan terhadap ketentuan hukum dan standar nasional yang mengatur pengelolaan data kesehatan.

Dalam lingkup pengaturan dan tata kelola rumah sakit, RSUD Serpong Utara telah membentuk unit khusus yang bertanggung jawab atas penyelenggaraan Rekam Medis Elektronik (RME), dengan struktur organisasi dan kewenangan yang ditetapkan melalui Surat Keputusan (SK). Pembagian tugas dalam unit ini disusun secara sistematis,

mencakup pengaturan hak akses, pemantauan aktivitas pengguna, serta koordinasi antarunit, sehingga proses pengelolaan data pasien dapat berjalan aman dan efisien. Sistem RME yang diterapkan berbasis SIMGOS dilengkapi dengan prosedur operasional standar (SOP) mengenai pencatatan, pengumpulan, penyimpanan, dan pembaruan data.

Keamanan data pasien dijaga melalui penyimpanan pada server eksternal, yaitu server yang dikelola di luar lingkungan rumah sakit oleh instansi atau penyedia layanan yang memiliki standar keamanan tinggi, sehingga memastikan integritas dan perlindungan data secara optimal. Selain itu, hak akses dibatasi dan setiap petugas menggunakan akun pribadi untuk mengakses sistem. Layanan rujukan pasien dilaksanakan menggunakan Sistem Informasi Jejaring Rujukan Terintegrasi (SISRUTE). Secara keseluruhan, langkah-langkah tersebut mencerminkan komitmen rumah sakit dalam menjaga kerahasiaan data pasien sebagai bagian dari upaya pencegahan kebocoran informasi medis.

Perlindungan kerahasiaan data pasien di RSUD Serpong Utara dilakukan melalui mekanisme persetujuan tertulis, pembatasan akses komunikasi, dan koordinasi berjenjang antara HUMAS, pimpinan, dan tenaga kesehatan. Meskipun mekanisme perlindungan kerahasiaan data pasien telah diterapkan, penyelenggaraan Rekam Medis Elektronik (RME) di RSUD Serpong Utara masih menghadapi sejumlah tantangan terkait transisi dari sistem manual ke digital. Implementasi Rekam Medis Elektronik (RME) di RSUD Serpong Utara masih bersifat hybrid sehingga proses pengolahan data antarunit memerlukan koordinasi yang lebih intensif.

Selain itu, belum adanya unit hukum internal dan Pejabat Perlindungan Data Pribadi membuat mekanisme formal untuk menangani potensi pelanggaran atau penyalahgunaan data pasien belum tersedia secara lengkap, sehingga pelatihan formal bagi petugas mengenai sanksi hukum berdasarkan seluruh peraturan yang mengatur perlindungan data pasien menjadi semakin penting untuk memperkuat pemahaman terhadap konsekuensi kebocoran data.

Sejalan dengan hal tersebut, pengelolaan CPPT (Catatan Perkembangan Pasien Terintegrasi) yang memuat data pribadi pasien juga menjadi tantangan. Sistem CPPT telah diperbarui agar tidak dapat disimpan bila elemen SOAP belum lengkap dan dikunci setelah finalisasi. Namun, data masih dapat dibuka tanpa meninggalkan jejak, sehingga audit trail belum sepenuhnya efektif. Komite Mutu terus melakukan evaluasi rutin berdasarkan indikator mutu, tetapi audit kepatuhan terhadap SOP dan keamanan data masih terbatas, serta kepatuhan SDM terhadap SOP dan pengaturan hak akses masih perlu ditingkatkan.

Analisis kepatuhan terhadap upaya pencegahan kebocoran data Rekam Medis Elektronik dilakukan dengan menilai kesesuaian antara praktik pengelolaan data pasien dan ketentuan hukum yang mengatur perlindungan data pribadi serta kerahasiaan informasi kesehatan. Berdasarkan hasil penelitian yang telah dilakukan, di bawah ini merupakan uraian analitis mengenai tingkat kepatuhan pengelolaan Rekam Medis Elektronik di RSUD Serpong Utara berdasarkan ketentuan hukum yang berlaku.

1. **Kepatuhan Berdasarkan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi**

   Perlindungan data pasien dalam UU PDP menegaskan bahwa rekam medis elektronik merupakan data pribadi sebagaimana dimaksud Pasal 1 Ayat 1, dan termasuk data pribadi spesifik yang memerlukan perlindungan paling tinggi

menurut Pasal 4 Ayat 2. Oleh karena itu, seluruh pengumpulan, penyimpanan, pemutakhiran, dan penghapusan data kesehatan wajib dilakukan secara terbatas, dan dilindungi dari akses yang tidak sah sesuai Pasal 16 [10].

Temuan di RSUD Serpong Utara menunjukkan bahwa rumah sakit telah menerapkan mekanisme pembatasan akses berbasis akun personal, pengaturan kewenangan sesuai jabatan, serta penyimpanan data pada server eksternal yang memenuhi prinsip keamanan, integritas, dan ketersediaan sebagaimana dijelaskan dalam Pasal 16 Ayat 2 huruf e [10].

Namun, beberapa kewajiban normatif belum sepenuhnya dipenuhi. Rumah sakit belum menunjuk Pejabat Pelindungan Data Pribadi sebagaimana diwajibkan Pasal 53 Ayat 1 [10], sehingga fungsi pengawasan dan evaluasi risiko belum berjalan optimal. Selain itu, belum terdapat prosedur audit insiden yang terstruktur, sementara Pasal 20 mensyaratkan setiap pemrosesan data harus memiliki dasar hukum yang jelas serta akuntabilitas yang dapat dipertanggungjawabkan [10][11]. Kelemahan lain terlihat pada sistem audit trail CPPT yang belum sepenuhnya mencatat jejak akses, sehingga berpotensi bertentangan dengan prinsip keamanan Pasal 16 dan larangan akses tanpa hak dalam Pasal 65 [10].

Secara keseluruhan, RSUD Serpong Utara telah memenuhi sebagian aspek teknis perlindungan data pribadi, namun kepatuhan struktural dan substantif masih perlu diperkuat agar penyelenggaraan RME benar-benar selaras dengan ketentuan UU PDP.

2. Kepatuhan Berdasarkan UU Nomor 11 Tahun 2008 jo. UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

UU ITE memberikan dasar hukum bagi perlindungan informasi elektronik, termasuk data kesehatan dalam rekam medis elektronik [19]. Pasal 27A melarang penyebaran informasi elektronik yang dapat merugikan kehormatan seseorang, sehingga kebocoran data pasien dipandang sebagai pelanggaran terhadap martabat dan privasi individu. Pasal 40 ayat 2 mewajibkan penyelenggara sistem elektronik untuk melakukan pencegahan dan pemutusan akses terhadap informasi yang melanggar hukum, yang berarti rumah sakit harus memiliki sistem pengamanan yang efektif dan terpantau [13].

RSUD Serpong Utara telah menerapkan sistem akses berbasis akun individual dan pengaturan hak akses sesuai kebutuhan kerja. Namun, temuan lapangan menunjukkan adanya kelemahan pada audit trail, khususnya pada CPPT yang belum merekam aktivitas pengguna secara komprehensif. Kondisi ini menyebabkan potensi akses tidak sah sulit terdeteksi dan menunjukkan bahwa mekanisme pencegahan belum bekerja secara optimal sebagaimana dijelaskan dalam Pasal 40 ayat 2 UU ITE [13].

Dengan demikian, kepatuhan RSUD Serpong Utara terhadap ketentuan UU ITE dapat dinilai sebagian terpenuhi. Beberapa elemen teknis sudah diimplementasikan, tetapi penguatan audit keamanan dan pencatatan aktivitas elektronik masih diperlukan untuk memenuhi standar perlindungan informasi elektronik secara menyeluruh.

3. Kepatuhan Berdasarkan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

PP No. 71 Tahun 2019 mengatur kewajiban penyelenggara sistem elektronik untuk menjaga keamanan, kerahasiaan, dan integritas data, serta meminimalkan risiko gangguan atau kerugian [14]. Di RSUD Serpong Utara, data RME disimpan pada server eksternal dengan standar keamanan tinggi dan hak akses dibatasi sesuai jabatan, sehingga sebagian kewajiban keamanan sistem sesuai Pasal 24 ayat 1 dan Pasal 31 telah terpenuhi [14].

Namun, pengelolaan CPPT masih memungkinkan data diakses tanpa meninggalkan rekam jejak, sehingga prinsip kerahasiaan dan keteraksesan data sebagaimana diatur dalam Pasal 26 ayat 1 belum sepenuhnya diterapkan [14].

4. Kepatuhan Berdasarkan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis

RSUD Serpong Utara telah menerapkan Rekam Medis Elektronik (RME) dengan membentuk unit khusus pengelola RME dan menggunakan platform SIMGOS, sesuai ketentuan Pasal 6–8 dan Pasal 21 Permenkes Nomor 24 Tahun 2022 [4]. Struktur unit ini mengatur hak akses, koordinasi antarunit, serta pemantauan aktivitas pengguna. Data pasien disimpan di server eksternal dengan standar keamanan tinggi, dan prosedur operasional standar (SOP) terkait pencatatan, penyimpanan, dan pembaruan data telah diterapkan. Upaya pencegahan kebocoran dilakukan melalui pembatasan hak akses, penggunaan akun pribadi, prosedur persetujuan tertulis, serta pengawasan oleh Kominfo sebagai pengelola server eksternal [5].

5. Kepatuhan Berdasarkan UU Nomor 17 Tahun 2023 tentang Kesehatan

Peraturan ini menegaskan hak pasien atas kerahasiaan informasi kesehatan dan akses terhadap rekam medis, serta menetapkan tanggung jawab tenaga medis, pimpinan fasilitas kesehatan, dan Kementerian Kesehatan dalam pengelolaan data sesuai Pasal 4 ayat 1 huruf i, Pasal 276, Pasal 296 ayat 5, Pasal 297, dan Pasal 298 [12].

Berdasarkan temuan lapangan, RSUD Serpong Utara telah menerapkan pembatasan akses dan koordinasi berjenjang antarunit dalam pengelolaan data pasien. Layanan rujukan menggunakan SISRUTE dan hak akses manual terlindungi, sehingga sebagian kewajiban pemenuhan hak pasien telah terpenuhi. Namun, tantangan tetap muncul pada catatan perkembangan pasien yang belum sepenuhnya memiliki audit trail, sehingga diperlukan penguatan mekanisme formal untuk memastikan semua akses dan perubahan data tercatat secara akurat.

Risiko Hukum Apabila Terjadi Kebocoran Data Rekam Medis Elektronik di RSUD Serpong Utara

Risiko hukum merujuk pada potensi timbulnya tanggung jawab yuridis yang harus ditanggung oleh suatu pihak akibat kegagalan memenuhi kewajiban hukum (Nadiroh & Wiraguna, 2025). Dalam ranah pelayanan kesehatan, kebocoran rekam medis elektronik dapat menimbulkan risiko hukum karena informasi medis dikategorikan sebagai data pribadi yang bersifat sangat sensitif (Budiman et al., 2025).

Penilaian risiko hukum terkait kebocoran rekam medis digital harus merujuk pada berbagai regulasi yang saling berkaitan seperti Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis, Undang-Undang No. 17 Tahun 2023 Kesehatan, dan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi rujukan utama karena mengatur kewajiban perlindungan kerahasiaan, keamanan, dan pemrosesan data medis yang bersifat sensitif (Hadiyantina Shinta et.al., 2023).

Regulasi tersebut diperkuat oleh Undang-Undang No. 11 Tahun 2008 Jo UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) yang memberikan standar keamanan sistem elektronik. Secara keseluruhan, ketentuan tersebut menunjukkan bahwa kebocoran data tidak hanya melanggar privasi pasien, tetapi juga mencerminkan kegagalan pemenuhan kewajiban pengamanan sistem.

Dalam hal ini RSUD Serpong Utara berperan sebagai Pengendali Data Pribadi dan penyelenggara sistem elektronik yang harus memastikan keamanan data, kepatuhan prosedur, dan penanganan insiden secara cepat. Kelalaian dalam menjalankan kewajiban tersebut berpotensi menimbulkan risiko hukum baik yang bersifat administratif, risiko hukum perdata, maupun risiko hukum pidana.

Pengelolaan rekam medis digital yang tidak memenuhi standar perlindungan data berpotensi menimbulkan risiko hukum bagi fasilitas pelayanan kesehatan sebagai subjek yang bertanggung jawab atas pemrosesan data pasien. Kebocoran RME menandakan kegagalan dalam memenuhi kewajiban normatif yang diatur oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Akbar & Wicaksana, 2025).

Risiko administratif muncul apabila RSUD Serpong Utara tidak memenuhi prinsip pemrosesan data sebagaimana diatur dalam Pasal 16 dan Pasal 20 UU PDP. Pelanggaran prinsip ini dapat berakibat pada sanksi administratif seperti teguran tertulis, penghentian sementara pemrosesan data, penghapusan sebagian data, maupun denda yang signifikan. Selain dampak hukum, sanksi ini berpotensi memengaruhi reputasi rumah sakit, legalitas layanan, dan tingkat kepercayaan publik terhadap institusi.

Risiko pidana muncul apabila data pasien diakses, diungkapkan, atau digunakan oleh pihak yang tidak berwenang. Berdasarkan Pasal 65 dan Pasal 67 UU PDP, pelanggaran dapat dikenai sanksi pidana berupa penjara atau denda. Misalnya, pengumpulan data pribadi secara ilegal dapat dihukum maksimal 5 tahun penjara atau denda Rp5 miliar, pengungkapan data tanpa izin maksimal 4 tahun penjara atau denda Rp4 miliar, dan penggunaan data pribadi secara ilegal maksimal 5 tahun penjara atau denda Rp5 miliar. Pertanggungjawaban pidana dapat dikenakan kepada individu pelaku, termasuk pegawai rumah sakit, tenaga kesehatan, personel IT, atau pihak ketiga, terutama bila terdapat kelalaian serius dalam pengawasan dan pengendalian akses.

Selain sanksi administratif dan pidana, Pasal 12 ayat (1) UU PDP memberikan hak kepada pasien sebagai subjek data untuk menuntut ganti rugi perdata apabila terjadi

pelanggaran pemrosesan data. Ganti rugi tersebut dapat berupa kerugian materiil, seperti dampak ekonomi akibat penyalahgunaan identitas, biaya tambahan akibat akses ilegal terhadap data, atau transaksi layanan kesehatan tanpa izin. Selain itu, terdapat kerugian immateriil, termasuk tekanan psikologis, rasa malu, hilangnya martabat, dan terganggunya privasi akibat bocornya informasi medis sensitif (Rizza Ayda, 2022).

Dengan demikian, kebocoran Rekam Medis Elektronik (RME) di RSUD Serpong Utara membuka ruang bagi pasien untuk mengajukan gugatan perbuatan melawan hukum (Pasal 1365 KUHPerdata) dan menuntut ganti rugi baik materiil maupun immateriil, dengan legitimasi hukum yang jelas berdasarkan UU PDP terhadap tanggung jawab pengendali data.

Selain risiko hukum yang timbul dari pelanggaran kewajiban perlindungan data pasien, penyelenggaraan Rekam Medis Elektronik di rumah sakit juga harus dipahami dalam kerangka pengaturan sektor kesehatan sebagaimana diatur dalam Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. Permenkes ini merupakan regulasi teknis yang secara spesifik mengatur penyelenggaraan Rekam Medis Elektronik (RME) di rumah sakit. Pasal 29 ayat (1) mengatur prinsip keamanan (security), integritas, dan ketersediaan data. Kegagalan rumah sakit dalam menerapkan prinsip ini dapat menimbulkan risiko hukum dan administratif, termasuk evaluasi sistem, pembatasan kerja sama dengan vendor, serta upaya pemulihan yang ditetapkan oleh Kementerian Kesehatan (Siregar, 2024).

Berdasarkan Pasal 25 ayat 1 Permenkes 24 Tahun 2022, dokumen Rekam Medis Elektronik merupakan milik rumah sakit, sedangkan isi informasi tetap menjadi milik pasien. Rumah sakit bertanggung jawab penuh atas kerusakan, kehilangan, atau akses tidak sah terhadap data pasien. Kegagalan pengendalian akses, termasuk pemberian hak akses yang tidak tepat, tidak adanya pembatasan berbasis peran, atau kurangnya pengawasan aktivitas pengguna, menimbulkan tanggung jawab hukum langsung bagi RSUD Serpong Utara, yang dapat berupa ganti rugi, sanksi administratif, dan penilaian akreditasi negatif (Purnomo & Mashuri, 2025).

Selain risiko yang timbul dari kelalaian internal, Permenkes No. 24 Tahun 2022 juga mengatur bahwa kelalaian dalam pemberian hak akses pegawai, seperti memberikan akses terlalu luas, tidak menerapkan prinsip least privilege principle atau tidak mengawasi jejak audit login, menimbulkan tanggung jawab hukum sesuai Pasal 30. Dalam kondisi ini, RSUD dapat dikenai teguran dari pemerintah, tuntutan pasien, serta konsekuensi etik dan disipliner bagi tenaga medis.

Selain itu, apabila rumah sakit bekerja sama dengan pihak ketiga dalam penyimpanan data pasien tanpa menyertakan pakta integritas atau perjanjian kerahasiaan sebagaimana diwajibkan Pasal 22 ayat 4 Permenkes 24 Tahun 2022, maka kebocoran data tetap menjadi tanggung jawab rumah sakit. Ketiadaan dokumen tersebut menunjukkan kelalaian administratif dalam pengendalian keamanan data. Pasal 22 ayat 3 juga menegaskan larangan bagi penyelenggara sistem elektronik untuk membuka atau memanfaatkan data secara tidak sah, dan rumah sakit tetap wajib memastikan pengawasan serta akses penuh terhadap data sebagaimana ditetapkan Pasal 22 ayat 5.

Risiko hukum juga muncul dalam mekanisme interoperabilitas nasional, terutama saat pengiriman data pasien ke Kementerian Kesehatan melalui sistem bridging (Ariani et

al., 2025). Kebocoran pada tahap ini tetap menimbulkan pertanggungjawaban bagi rumah sakit karena kewajiban pengendalian data tidak dapat dialihkan.

Dalam kerangka perlindungan hukum yang lebih komprehensif, risiko hukum atas kebocoran data pasien juga harus dilihat dalam kerangka perlindungan hak pasien yang dijamin secara langsung dalam Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan yang menempatkan perlindungan data kesehatan sebagai bagian dari hak pasien dan memiliki kekuatan hukum langsung. Pasal 4 ayat 1 huruf i menegaskan bahwa setiap orang berhak atas kerahasiaan data kesehatannya, sedangkan Pasal 276 memberikan hak bagi pasien untuk memperoleh informasi medis dan mengakses data yang terdapat dalam rekam medis.

Dengan demikian, setiap insiden kebocoran data berpotensi menimbulkan risiko hukum bagi rumah sakit karena dianggap menghalangi hak pasien untuk mendapatkan privasi, transparansi informasi, dan kendali atas data kesehatannya (Lukitasari, Khoirul Huda, 2023).

Tanggung jawab hukum rumah sakit diperkuat melalui Pasal 296, Pasal 297, dan Pasal 298 UU Nomor 17 Tahun 2023 tentang Kesehatan, yang menegaskan kewajiban tenaga kesehatan dan fasilitas pelayanan kesehatan menjaga kerahasiaan, keamanan, keutuhan, dan ketersediaan data rekam medis.

Kementerian Kesehatan sebagai pihak yang bertanggung jawab atas pengelolaan data rekam medis secara nasional, mulai dari kebijakan, penyimpanan, pengamanan, hingga transfer dan pengawasan sebagaimana dijelaskan dalam Pasal 298, menunjukkan bahwa rumah sakit wajib memastikan sistem keamanan informasi yang selaras dengan kebijakan nasional. Kegagalan memenuhi standar tersebut berpotensi menimbulkan risiko administratif, perdata, maupun etis bagi RSUD Serpong Utara apabila terjadi kebocoran data.

Selain pengaturan hukum di bidang kesehatan, pengelolaan Rekam Medis Elektronik juga berada dalam ruang lingkup sistem informasi digital yang tunduk pada Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, sehingga setiap kelemahan dalam pengamanan dan pengendalian sistem berpotensi menimbulkan risiko hukum bagi penyelenggara layanan kesehatan.

Informasi medis yang bersifat sensitif seperti status riwayat penyakit tertentu atau data lain yang berpotensi menurunkan martabat pasien dapat dikategorikan sebagai pelanggaran kehormatan sebagaimana dimaksud dalam Pasal 27A UU ITE. Kebocoran semacam ini memberi dasar bagi pasien untuk mengajukan tuntutan pidana maupun gugatan perdata karena dianggap merugikan nama baik dan kehormatan akibat kelalaian fasilitas pelayanan kesehatan sebagai penyelenggara sistem elektronik.

Pemerintah memiliki kewenangan untuk memerintahkan pemutusan akses atau penghentian layanan apabila sistem elektronik dianggap membahayakan keamanan data sebagaimana dijelaskan dalam Pasal 40. Jika tindakan tersebut mencapai sistem rekam medis digital, konsekuensinya tidak hanya berupa tanggung jawab hukum bagi rumah sakit, tetapi juga gangguan langsung terhadap layanan operasional. Dengan demikian, risiko hukum menurut UU ITE mencakup sanksi pidana, perdata, serta risiko terhentinya

layanan kesehatan akibat intervensi pemerintah terhadap sistem elektronik yang tidak aman.

Pengaturan risiko hukum dalam Undang-Undang Informasi dan Transaksi Elektronik tersebut selanjutnya dipertegas melalui peraturan pelaksana dalam PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang mengatur kewajiban penyelenggara sistem elektronik dan tata kelola pengelolaan data secara normatif, sehingga memberikan kerangka hukum yang lebih operasional dalam menilai risiko hukum atas pengelolaan data digital.

Apabila terjadi kebocoran, hal tersebut menunjukkan kegagalan RSUD Serpong Utara dalam memenuhi kewajiban pengamanan sebagaimana ditetapkan dalam Pasal 24 dan Pasal 26. Konsekuensinya dapat berupa teguran tertulis, perintah perbaikan sistem, pembatasan layanan, penghentian sementara operasional modul tertentu, hingga denda administratif serta evaluasi regulator apabila kerugian dialami pasien sebagaimana diatur dalam Pasal 31.

Risiko hukum juga muncul apabila kebocoran melibatkan pihak ketiga karena rumah sakit tetap bertanggung jawab apabila tidak memiliki mekanisme pengawasan atau perjanjian perlindungan data yang memadai. Selain itu, Pasal 15 menegaskan prinsip pembatasan penyimpanan data, sehingga apabila rumah sakit tetap menyimpan data pasien yang sudah tidak relevan lagi dan kemudian data tersebut mengalami kebocoran, hal ini dapat dianggap sebagai bentuk kelalaian yang menimbulkan sanksi administratif maupun gugatan perdata.

KESIMPULAN

Berdasarkan hasil penelitian, upaya pencegahan kebocoran data rekam medis elektronik pasien di RSUD Serpong Utara telah dilakukan melalui mekanisme pembatasan akses, penggunaan akun personal, pengawasan berjenjang, dan penyimpanan data pada server eksternal. Namun, implementasi masih belum menyeluruh karena unit rawat inap dan IGD masih menggunakan sistem hybrid, audit trail CPPT belum efektif, serta belum adanya Pejabat Perlindungan Data Pribadi dan unit hukum internal. Kondisi ini menunjukkan bahwa aspek struktural dan substantif kepatuhan hukum belum sepenuhnya terpenuhi, sehingga upaya pencegahan kebocoran data rekam medis elektronik belum sepenuhnya memenuhi standar yang ditetapkan dalam UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, UU Nomor 17 Tahun 2023 tentang Kesehatan, UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis.

Kelemahan dalam implementasi RME menimbulkan risiko hukum sebagai berikut:

1. **Risiko Hukum Administratif**
   Rumah sakit berpotensi menerima sanksi berupa teguran tertulis, penghentian sementara pemrosesan data, penghapusan sebagian data, pembatasan layanan, atau denda hingga 2% dari pendapatan tahunan akibat kegagalan memenuhi prinsip pemrosesan data (Pasal 16 dan Pasal 20 UU PDP) dan kewajiban pengamanan sistem elektronik (Pasal 24 dan Pasal 31 PP 71/2019).
2. **Risiko Hukum Perdata**
   Pasien sebagai subjek data dapat mengajukan gugatan ganti rugi materiil (dampak ekonomi, biaya tambahan, transaksi tanpa izin) dan immateriil (tekanan psikologis,

rasa malu, hilangnya martabat, gangguan privasi) berdasarkan Pasal 1365 KUHPerdata tentang perbuatan melawan hukum dan Pasal 12 UU PDP.

3. **Risiko Hukum Pidana**
   Individu pelaku (pegawai rumah sakit, tenaga kesehatan, personel IT, atau pihak ketiga) dapat dikenakan sanksi pidana berupa penjara dan/atau denda apabila terjadi akses atau penggunaan data tidak sah, antara lain: pengumpulan data pribadi ilegal (maksimal 5 tahun penjara atau denda Rp5 miliar), pengungkapan data tanpa izin (maksimal 4 tahun penjara atau denda Rp4 miliar), dan penggunaan data pribadi ilegal (maksimal 5 tahun penjara atau denda Rp5 miliar) berdasarkan Pasal 65 dan Pasal 67 UU PDP, serta Pasal 45 ayat 3 UU ITE.

Berdasarkan temuan penelitian, direkomendasikan langkah-langkah strategis sebagai berikut:

1. **Penunjukan Pejabat Perlindungan Data Pribadi (DPO)**
   Menunjuk DPO sesuai Pasal 53 UU PDP untuk mengawasi kepatuhan regulasi, melakukan evaluasi berkala sistem RME, dan menangani pengaduan pelanggaran data.
2. **Pelaksanaan Data Protection Impact Assessment (DPIA)**
   Melakukan DPIA sesuai Pasal 34 UU PDP untuk memetakan alur data, mengevaluasi kelemahan sistem keamanan, dan menyusun rencana mitigasi risiko terukur.
3. **Pembentukan Unit Hukum Internal**
   Membentuk unit hukum internal untuk memberikan legal advisory, menangani sengketa, menyusun perjanjian dengan pihak ketiga, dan menyusun SOP penanganan insiden kebocoran data.
4. **Penuntasan Transisi Digital Menyeluruh**
   Menyelesaikan implementasi RME di seluruh unit (rawat inap dan IGD) dengan dukungan infrastruktur memadai, pelatihan intensif, dan evaluasi kesiapan sistem berkala.
5. **Implementasi Audit Trail Efektif pada CPPT**
   Mengimplementasikan sistem audit trail yang merekam identitas pengguna, waktu akses, jenis aktivitas, dan perubahan data secara otomatis dan terintegrasi dengan monitoring keamanan real-time.
6. **Penyusunan Prosedur Audit Insiden Terstruktur**
   Menyusun prosedur audit insiden yang mencakup deteksi dini, pelaporan, investigasi, mitigasi, protokol komunikasi krisis, dan pemberitahuan kepada pasien terdampak sesuai Pasal 62 UU PDP.
7. **Pelatihan Rutin dan Sertifikasi Kompetensi**
   Melaksanakan pelatihan komprehensif bagi petugas mengenai keamanan data, regulasi perlindungan data, konsekuensi hukum pelanggaran, dan prosedur penanganan insiden, disertai sertifikasi kompetensi.
8. **Penguatan Perjanjian dengan Pihak Ketiga**
   Memperkuat perjanjian kerahasiaan dengan pengelola server eksternal dan vendor IT sesuai Pasal 22 ayat 4 Permenkes 24/2022, mengatur kewajiban perlindungan data dan hak audit rumah sakit.

9. **Evaluasi dan Pembaruan Kebijakan Berkala**
   Melakukan evaluasi kebijakan keamanan data minimal setiap enam bulan sekali dengan melibatkan DPO, unit hukum internal, tim IT, Komite Mutu, dan manajemen puncak.

DAFTAR REFERENSI

[1] Agustina Tifanny. (2025). *Era Baru Kesehatan: Digitalisasi dan Integrasi Data Untuk Pelayanan Optimal* (Rerung R (ed.)). CV. Media Sains Indonesia. https://kbk1773719.perpustakaandigital.com/detail/era-baru-kesehatan-digitalisasi-dan-integrasi-data-untuk-pelayanan-optimal

[2] Wijayanta Setya. (2024). *Electronic Health Records*. CV Media Sains Indonesia.

[3] Neng Sari Rubiyanti. (2023). Penerapan Rekam Medis Elektronik di Rumah Sakit di Indonesia: Kajian Yuridis. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, 1(1), 179–187. https://doi.org/10.59246/aladalah.v1i1.163

[4] Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 Tentang Rekam Medis, 1 (2022).

[5] Siregar, R. A. (2024). Penerapan Permenkes Nomor 24 Tahun 2022 Tentang Rekam Medis Terhadap Efektivitas Pelayanan Kesehatan. *Jurnal Ilmu Hukum Kyadiren*, 5(2), 1–12. https://doi.org/10.46924/jihk.v5i2.182

[6] Ariani, S., Yuliani, R. D., & Sidoarjo, U. M. (2025). Tantangan dalam Integrasi Data Kesehatan dari Berbagai Sistem Electronic Health Record dalam Sistem Kesehatan Nasional Universitas Muhammadiyah Sidoarjo, Indonesia Rekam Medis Elektronik (Electronic Health Records/EHR) telah menjadi.

[7] Izza, A. Al, & Lailiyah, S. (2024). Kajian Literatur: Gambaran Implementasi Rekam Medis Elektronik di Rumah Sakit Indonesia berdasarkan Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis. *Media Gizi Kesmas*, 13(1), 549–562. https://doi.org/10.20473/mgk.v13i1.2024.549-562

[8] Juliansyah, R. (2025). Implementation of EMR System in Indonesian Health Facilities: Benefits and Constraints – A Case Study of Two Clinics in Central Java. 10(1). https://doi.org/10.7454/ihpa.v10i1.1140

[9] Hadiyantina Shinta et.al. (2023). *Perlindungan Data Pribadi Dalam Bidang Rekam Medis*.Ub Media Press. https://books.google.co.id/books?hl=en&id=C1LyEAAAQBAJ&lr=&oi=fnd&ots=y3TZMp8yLU&pg=PR4&redir_esc=y&sig=z5USCf1-_rz05QzoBFSNviWKhxE&utm

[10] Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (2022). https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

[11] Akbar, H., & Wicaksana, P. B. (2025). Perlindungan Hukum Terhadap Kebocoran Data Pribadi Akibat Tindak Pidana Siber: Perspektif Undang-Undang Nomor 27 Tahun 2022. 18(02), 239–248.

[12] Undang-Undang (UU) Nomor 17 Tahun 2023 Tentang Kesehatan (2023). https://peraturan.bpk.go.id/details/258028/uu-no-17-tahun-2023

[13] Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 44 *Journal of Physics A: Mathematical and Theoretical* 287 (2011). https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016

[14] Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (2016).

[15] Tovino A. (2022). Health Privacy, Security, and Information Management. In *in Laws of Medicine: Core Legal Aspects for the Healthcare Professional*. Springer. https://doi.org/https://doi.org/10.1007/978-3-031-08162-0
[16] Gede, I., Agung, E., & Punia, A. (2024). Aspek Hukum Dan Pertanggungjawaban Keamanan Data Rekam Medis Elektronik Di Indonesia. *Jurnal Kesehatan Mahasaraswati*, 1, 1–4.
[17] Budiman, A., Isa, M., & Soekiswati, S. (2025). Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RS P Surakarta (Vol. 7, Issue 3).
[18] Nadiroh, A., & Wiraguna, S. A. (2025). Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia. 2(6), 313–320.
[19] Mandey, A. W. (2025). Legal Analysis of Patient Privacy Violation in Electronic Medical Records and its Implications for Health Data Protection in Indonesia. 5(02), 589–594. https://doi.org/10.58471/jms.v5i02
[20] Tatang Guritno, K. (2022). Kemkominfo Telusuri Dugaan Kebocoran Data Pasien Milik Kemenkes Artikel ini telah tayang di Kompas.com dengan judul "Kemkominfo Telusuri Dugaan Kebocoran Data Pasien Milik Kemenkes", Klik untuk baca: https://nasional.kompas.com/read/2022/01/06/22555491/ke. *Kompas.Com*. https://nasional.kompas.com/read/2022/01/06/22555491/kemkominfo-telusuri-dugaan-kebocoran-data-pasien-milik-kemenkes?
[21] Rizza Ayda. (2022). Perlindungan Hukum Terhadap Data Rekam Medis Pasien Covid-19 Di Rumah Sakit.
[22] Purnomo, A., & Mashuri, M. (2025). Data Rekam Medis Pasien. 9.
[23] Fadila Aprilia & Pranoto Edi. (2023). Analisis Hukum Terhadap Pelaksanaan Perlindungan Data Pribadi Pasien Dalam Sistem Rekam Medis Elektronik.
[24] Kurniawan, A. L., & Setiawan, A. (2021). Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi Covid-19. 9, 95–112.
[25] Ulfa Nadiya & Yuspin Wardah. (2022). Legality of Electronic Medical Records (RME) in Hospital Management Information System Readiness based on Minister of Health Regulation Number 24 of 2022 concerning Medical Records. 24, 72–78.
[26] Kusumastuti Adhi, M. A. (2019). *METODE PENELITIAN KUALITATIF* (Annisya Fitratun (ed.)). LEMBAGA PENDIDIKAN SUKARNO PRESSINDO. https://lib.unnes.ac.id/40372/1/Metode Penelitian Kualitatif.pdf
[27] Lukitasari, & Khoirul Huda. (2023). Perlindungan Hukum Hak Privasi Pasien dalam Pelayanan Kesehatan. *Jurnal Hukum Kesehatan Indonesia*, 12(2), 45–58.