Jurnal Cendekia Hukum Indonesia
Vol. 2 No. 1 April 2026
Licensed CC BY-SA 4.0, Hal 777-786
DOI: https://doi.org/10.71417/jchi.v2i1.176
https://hukum.journalpustakacendekia.com/index.php/JCHI

Integration of Electronic Medical Records in The Satusehat Ecosystem: Synchronizing Regulations and Legal Challenges of Protecting Medical Data from Cyber Threats

Dinda Marshanda Aurora
Universitas Komputer Indonesia, Bandung

Wahyudi
Universitas Komputer Indonesia, Bandung

Alamat: Jl. Dipati Ukur No. 112–116, Lebakgede, Kecamatan Coblong, Kota Bandung, Jawa Barat 40132, Indonesia.

Korespondensi penulis: dinda.31622002@mahasiswa.unikom.ac.id

Abstract. *The digital transformation of the Indonesian healthcare sector, as affirmed by Law No. 17 of 2023 concerning Health and Minister of Finance Regulation No. 24 of 2022, requires all healthcare facilities to switch to using Electronic Medical Records (EMDR). This policy is based on the principle that the right to confidentiality of personal health data is a fundamental right of every individual that must be safeguarded. However, the integration of medical data into digital systems creates a high vulnerability to cyberattacks that pose a risk to both patients and hospitals. Using a sociological-juridical approach and analytical-descriptive specifications, this study aims to evaluate the extent to which existing regulations provide legal certainty regarding medical data confidentiality and identify legal challenges in mitigating cyber data protection failures. As a case study, Budi Rahayu General Hospital has implemented patient rights protection through internal regulations that regulate access restrictions, the use of confidential user IDs and passwords, and the security of the SIMRS system through a firewall and an unpublished local server IP address. Although no data leaks had occurred up to the time of the study, real obstacles were still found in its implementation, such as rarely changing passwords, the presence of autofill features, lack of operational staff capabilities, unclear vendor access restrictions, low patient knowledge of their rights, and an EMR system that did not yet have full interoperability capabilities.*

Keywords: *Electronic Medical Records, Personal Data Protection, Cybersecurity, Patient Rights, Risk Mitigation*

Abstrak. Transformasi digital dalam sektor kesehatan di Indonesia, yang dipertegas melalui UU No. 17 Tahun 2023 tentang Kesehatan dan PMK No. 24 Tahun 2022, mewajibkan seluruh fasilitas pelayanan kesehatan beralih menggunakan Rekam Medis Elektronik (RME). Kebijakan ini didasari pada prinsip bahwa hak atas kerahasiaan data kesehatan pribadi merupakan hak asasi setiap individu yang harus dijaga keamanannya. Namun, integrasi data medis ke dalam sistem digital menciptakan kerentanan tinggi terhadap ancaman serangan siber yang berisiko merugikan pasien maupun rumah sakit. Melalui metode pendekatan yuridis sosiologis dan spesifikasi deskriptif analitis, penelitian ini bertujuan mengevaluasi sejauh mana regulasi yang ada mampu memberikan kepastian hukum terhadap kerahasiaan data medis serta mengidentifikasi tantangan yuridis dalam mitigasi kegagalan perlindungan data siber. Sebagai studi kasus, RSU Budi Rahayu telah menerapkan perlindungan hak pasien melalui regulasi internal yang mengatur batasan hak akses, penggunaan user ID dan kata sandi rahasia, serta pengamanan sistem SIMRS melalui firewall dan IP address server lokal yang tidak dipublikasikan. Meskipun hingga penelitian dilakukan belum

Received Maret 05, 2026; Revised Maret 12, 2026; Accepted Maret 20, 2026
*Dinda Marshanda Aurora, *dinda.31622002@mahasiswa.unikom.ac.id*

terjadi kebocoran data, masih ditemukan hambatan nyata dalam pelaksanaannya, seperti kata sandi yang jarang diubah, adanya fitur autofill, kurangnya kemampuan operasional staf, ketidakjelasan batasan akses vendor, rendahnya pengetahuan pasien akan haknya, serta sistem RME yang belum sepenuhnya memiliki kemampuan interoperabilitas.

Kata Kunci: Hak Pasien, Keamanan Siber, Mitigasi Resiko, Perlindungan Data Pribadi, Rekam Medis Elektronik

LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah membawa transformasi fundamental dalam berbagai sektor kehidupan, termasuk sektor pelayanan kesehatan di Indonesia. Salah satu tonggak utama transformasi ini adalah migrasi dari sistem pendokumentasian manual menuju Rekam Medis Elektronik (RME). Transformasi digital di sektor kesehatan terbukti mampu meningkatkan efisiensi layanan, kualitas pengambilan keputusan klinis, serta integrasi data antar fasilitas kesehatan (Kruse et al., 2018; WHO, 2021). Berdasarkan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis, seluruh fasilitas pelayanan kesehatan diwajibkan untuk menyelenggarakan rekam medis elektronik paling lambat pada tanggal 31 Desember 2023. Kebijakan ini bertujuan untuk meningkatkan efisiensi, akurasi data, dan integrasi layanan kesehatan nasional melalui platform satu data kesehatan. Namun, di balik efisiensi yang ditawarkan, digitalisasi data medis menyimpan risiko yuridis yang sangat besar. Data medis bukan sekadar data pribadi biasa; dalam perspektif hukum internasional dan nasional, data medis dikategorikan sebagai data pribadi yang bersifat sensitif (sensitive personal data) yang memerlukan perlindungan khusus (Voigt & von dem Bussche, 2017; Greenleaf, 2020). Data ini mencakup riwayat penyakit, hasil laboratorium, hingga informasi genetik yang jika bocor dapat merugikan harkat, martabat, dan hak privasi pasien secara permanen.

Urgensi penelitian ini semakin nyata mengingat meningkatnya frekuensi serangan siber terhadap infrastruktur informasi vital di Indonesia. Laporan menunjukkan bahwa sektor kesehatan menjadi salah satu target utama serangan siber global karena tingginya nilai data medis di pasar gelap (Coventry & Branley, 2018; ENISA, 2022). Ancaman seperti ransomware, phishing, dan peretasan database telah menjadi risiko nyata bagi penyelenggara sistem elektronik. Ketika data medis pasien bocor ke ruang publik, konsekuensi hukumnya tidak hanya menyentuh aspek administratif, tetapi juga perdata dan pidana (Kementerian Kominfo, 2023). Lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebenarnya telah memberikan standar baru bagi proteksi data, namun implementasinya pada sistem RME di rumah sakit masih menghadapi berbagai tantangan kompleks, baik dari sisi kesiapan teknologi maupun kepatuhan hukum pengelola data (Suhartono, 2023). Selain itu, dalam konteks penegakan hukum, pengelolaan arsip digital ini juga menjadi krusial saat terjadi sengketa medis. Validitas dan keautentikan rekam medis elektronik sebagai alat bukti di persidangan harus memenuhi prinsip integritas, keandalan, dan non-repudiation (Casey, 2011). Ketidaksiapan dalam memitigasi kebocoran data siber dapat menyebabkan ketidakpastian hukum dan hilangnya kepercayaan publik terhadap sistem kesehatan digital.

Urgensi perlindungan data dalam sistem Rekam Medis Elektronik (RME) bukan sekadar isu teknis operasional, melainkan perwujudan dari amanat konstitusi mengenai perlindungan privasi individu sebagai bagian dari hak asasi manusia (UUD 1945 Pasal 28G). Dalam lanskap hukum Indonesia, transisi ini menciptakan titik temu sekaligus tantangan antara UU No. 17 Tahun 2023 tentang Kesehatan yang mendorong digitalisasi layanan, dengan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang menetapkan standar kepatuhan ketat bagi pengendali data. Data medis, yang diklasifikasikan sebagai data pribadi bersifat spesifik atau sensitif, memerlukan tingkat keamanan yang lebih tinggi karena kebocorannya dapat berdampak pada diskriminasi sosial, kerugian ekonomi, hingga trauma psikologis permanen bagi pasien (Mantelero, 2013; ICO, 2021). Oleh karena itu, penguatan kerangka hukum dan tata kelola data menjadi kebutuhan mendesak dalam menjamin perlindungan hak pasien di era digital.

Penerapan RME di fasilitas kesehatan seperti RSU Salamun menghadapi dilema antara kemudahan akses layanan (interoperability) dan ketahanan sistem keamanan. Di satu sisi, integrasi data melalui platform seperti SatuSehat bertujuan mewujudkan efisiensi layanan kesehatan nasional, namun di sisi lain setiap titik integrasi menjadi celah potensial bagi serangan siber seperti ransomware atau phishing yang kian marak mengincar sektor kesehatan (Kshetri, 2021). Risiko ini semakin diperparah oleh faktor internal, seperti rendahnya literasi digital staf medis dan belum optimalnya protokol pembaruan keamanan secara berkala (Kruse et al., 2017). Selain aspek keamanan teknis, validitas rekam medis elektronik sebagai alat bukti hukum dalam sengketa medik menjadi isu krusial yang perlu dikaji lebih dalam. Ketidakpastian mengenai integritas data digital saat terjadi peretasan tidak hanya mengancam hak privasi pasien, tetapi juga dapat melemahkan posisi hukum rumah sakit dalam proses litigasi. Oleh karena itu, diperlukan sinkronisasi yang kuat antara regulasi kesehatan dengan standar keamanan siber nasional guna menjamin bahwa transformasi digital ini tetap berpijak pada kepastian hukum dan perlindungan hak asasi manusia.

Kebaruan dan urgensi penelitian ini terletak pada integrasi analisis antara aspek hukum perlindungan data pribadi, keamanan siber, dan validitas pembuktian hukum dalam konteks implementasi Rekam Medis Elektronik di tingkat rumah sakit. Berbeda dengan penelitian sebelumnya yang cenderung berfokus pada aspek teknis atau kebijakan secara parsial, penelitian ini menawarkan pendekatan komprehensif yang mengaitkan implementasi UU PDP, regulasi kesehatan, serta praktik pengelolaan arsip digital dalam perspektif pembuktian hukum. Urgensinya semakin tinggi mengingat percepatan digitalisasi layanan kesehatan nasional yang tidak selalu diiringi dengan kesiapan infrastruktur keamanan dan kepatuhan hukum. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi nyata dalam merumuskan model perlindungan data medis yang tidak hanya aman secara teknis, tetapi juga kuat secara yuridis.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif (legal research) yang berfokus pada pengkajian penerapan kaidah atau norma dalam hukum positif terkait keselarasan regulasi perlindungan data medis dengan tantangan keamanan siber pada sistem Rekam Medis Elektronik (RME). Pendekatan yang digunakan meliputi pendekatan perundang-undangan (statute approach) untuk menelaah regulasi seperti UU PDP, UU Kesehatan, UU ITE, dan Permenkes No. 24 Tahun 2022, serta pendekatan konseptual (conceptual approach) yang merujuk pada doktrin hak atas privasi dan rahasia medis. Data yang diolah merupakan data sekunder yang terdiri dari bahan hukum primer (peraturan perundang-undangan), sekunder (jurnal, buku, dan laporan kasus), serta tersier (kamus hukum) yang dikumpulkan melalui studi kepustakaan (library research). Keseluruhan bahan hukum tersebut kemudian dianalisis secara deskriptif-kualitatif dengan interpretasi hukum dan penarikan kesimpulan secara deduktif untuk mengevaluasi sejauh mana hukum positif Indonesia mampu memberikan perlindungan terhadap kerahasiaan data medis di tengah ancaman siber.

HASIL DAN PEMBAHASAN

A. Kerangka Regulasi Pelindungan Data Medis dalam Sistem RME di Indonesia

Kajian mengenai perlindungan data medis dalam sistem RME tidak terlepas dari susunan hierarkis peraturan perundang-undangan yang saling terkait, yang mencakup berbagai tingkatan mulai dari Undang-Undang hingga Peraturan Menteri di bidang teknis.Transformasi digital ini dikukuhkan melalui UU No. 17 Tahun 2023 tentang Kesehatan dan PMK No. 24 Tahun 2022, yang mewajibkan seluruh fasyankes beralih ke sistem elektronik paling lambat 31 Desember 2023. Dasar kebijakan ini adalah prinsip bahwa hak atas kerahasiaan data kesehatan pribadi merupakan hak asasi manusia yang fundamental dan wajib dijaga keamanannya oleh negara serta penyelenggara layanan. engesahan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) secara fundamental mengubah lanskap hukum dengan menetapkan data kesehatan sebagai

Data Pribadi Spesifik. Status "spesifik" ini memberikan standar perlindungan tingkat tinggi (golden standard) karena kebocoran data medis dapat berdampak permanen pada harkat, martabat, dan privasi pasien, seperti stigmatisasi sosial atau diskriminasi ekonomi. Sebagai implikasinya, fasyankes kini memikul tanggung jawab imperatif sebagai Pengendali Data Pribadi yang wajib melakukan Penilaian Dampak Pelindungan Data (Data Protection Impact Assessment) untuk memitigasi risiko serangan siber secara dini.

Dalam aspek operasional, fasyankes juga tunduk pada UU ITE (UU No. 1 Tahun 2024) dan PP No. 71 Tahun 2019 (PP PSTE) sebagai Penyelenggara Sistem Elektronik (PSE). Regulasi ini mewajibkan fasyankes menjamin tiga pilar utama: ketersediaan (availability), keutuhan (integrity), dan kerahasiaan (confidentiality) data medis. Apabila terjadi kegagalan sistem yang mengakibatkan kebocoran data, fasyankes tidak hanya menghadapi sanksi administratif, tetapi juga potensi tuntutan perdata dan pidana jika terbukti lalai dalam menerapkan standar keamanan yang layak. Kewajiban ini dipertegas dengan keharusan mengelola rekam jejak elektronik (log audit) guna membuktikan validitas akses data dalam sengketa hukum atau sengketa medis. Terakhir, tata kelola data dalam ekosistem nasional melalui platform SATUSEHAT menciptakan struktur akuntabilitas baru. Berdasarkan PMK No. 24 Tahun 2022, sistem RME harus memiliki kemampuan interoperabilitas untuk terhubung dengan basis data pusat, namun tetap dengan protokol keamanan transmisi yang kuat guna mencegah intersepsi informasi. UU Kesehatan memperkuat "benteng yuridis" ini dengan menegaskan bahwa rahasia kesehatan pasien hanya boleh dibuka untuk kepentingan medis, permintaan aparat penegak hukum, atau kepentingan publik tertentu yang diatur undang-undang. Dengan demikian, integrasi data masif ini tetap harus berpijak pada kedaulatan subjek data melalui mekanisme persetujuan (consent management) yang transparan selaras dengan mandat UU PDP.

1. **Kedudukan Data Medis sebagai Data Pribadi Spesifik (UU PDP No. 27/2022)**

   Pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) secara fundamental mengubah lanskap pengaturan kerahasiaan informasi kesehatan di Indonesia. Melalui Pasal 4 ayat (2), undang-undang ini memberikan status khusus bagi data kesehatan sebagai Data Pribadi yang bersifat spesifik, yang membedakannya secara signifikan dari data pribadi bersifat umum. Klasifikasi ini didasarkan pada filosofi bahwa data medis mengandung informasi yang sangat sensitif terkait integritas jasmani dan rohani seseorang, sehingga kebocoran terhadap data ini berpotensi menimbulkan dampak yang jauh lebih fatal, mulai dari stigmatisasi sosial hingga diskriminasi dalam akses pekerjaan atau asuransi. Status spesifik ini menempatkan data kesehatan di bawah standar perlindungan "emas" (golden standard), di mana setiap aktivitas pemrosesan dalam ekosistem Rekam Medis Elektronik (RME) harus memenuhi kriteria keamanan siber yang berlapis.

   Implikasi hukum dari penetapan status data spesifik ini membebankan tanggung jawab yang lebih berat kepada Fasilitas Pelayanan Kesehatan (fasyankes) sebagai Pengendali Data Pribadi. Berdasarkan Pasal 31 UU PDP, fasyankes diwajibkan untuk melaksanakan Penilaian Dampak Pelindungan Data (Data Protection Impact Assessment) guna mengidentifikasi secara dini risiko-risiko dalam sistem elektronik yang mereka kelola. Hal ini menunjukkan bahwa perlindungan terhadap data medis tidak lagi sekadar kewajiban etik kedokteran, melainkan kewajiban teknis-yuridis yang bersifat imperatif. Dengan adanya UU PDP, pasien selaku subjek data memiliki posisi tawar yang lebih kuat untuk menuntut akuntabilitas fasyankes, terutama dalam hal pemenuhan hak atas privasi yang harus dijamin keberlangsungannya oleh negara di tengah pesatnya ancaman kebocoran data pada ruang digital.

2. **Kewajiban Digitalisasi dan Integritas Sistem (Permenkes No. 24 Tahun 2022)**

   Adopsi Rekam Medis Elektronik (RME) di Indonesia kini bukan lagi merupakan sebuah pilihan, melainkan kewajiban yuridis bagi seluruh fasilitas pelayanan kesehatan (fasyankes) sebagaimana diatur dalam Peraturan Menteri Kesehatan Nomor 24 Tahun 2022. Regulasi ini menetapkan batas waktu transisi digitalisasi yang ketat, yang bertujuan

untuk mewujudkan ekosistem data kesehatan nasional yang terintegrasi. Namun, inti dari Permenkes ini tidak hanya terletak pada peralihan media penyimpanan dari fisik ke digital, melainkan pada kewajiban fasyankes untuk menjamin integritas dan keamanan data secara berkesinambungan. Melalui standar interoperabilitas yang diwajibkan, setiap sistem RME harus mampu terhubung secara aman dengan platform SATUSEHAT, yang menuntut adanya protokol keamanan transmisi data yang kuat guna mencegah terjadinya intersepsi atau manipulasi informasi medis pasien di tengah jalan.

Aspek krusial lain dalam Permenkes No. 24 Tahun 2022 adalah penegasan mengenai tanggung jawab manajerial fasyankes terhadap kerahasiaan data elektronik. Berdasarkan ketentuan Pasal 28, pimpinan fasyankes memikul tanggung jawab penuh untuk memastikan bahwa data medis terlindungi dari akses yang tidak sah, kerusakan, maupun kehilangan. Hal ini mencakup implementasi sistem kendali akses yang ketat dan penggunaan teknologi enkripsi sebagai pelindung utama data sensitif. Mengingat kewajiban retensi data medis elektronik mencapai 25 tahun, regulasi ini secara tidak langsung mewajibkan fasyankes untuk memiliki strategi pemeliharaan infrastruktur digital yang resilien terhadap ancaman siber yang terus berevolusi. Dengan demikian, Permenkes ini memposisikan keamanan sistem informasi sebagai parameter utama dalam penilaian kualitas dan legalitas layanan kesehatan di era digital.

Salah satu tantangan yuridis yang muncul dalam implementasi Rekam Medis Elektronik (RME) adalah potensi antinomi norma antara Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dengan regulasi sektoral kesehatan. Pasal 43 UU PDP memberikan hak kepada subjek data untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadinya (right to erasure). Namun, di sisi lain, Pasal 28 Permenkes No. 24 Tahun 2022 menetapkan kewajiban retensi data medis elektronik selama 25 tahun untuk kepentingan pelayanan, hukum, dan penelitian. Ketidaksinkronan ini menciptakan ambiguitas bagi fasilitas pelayanan kesehatan (fasyankes) sebagai pengendali data. Jika fasyankes mengabulkan permintaan penghapusan data pasien demi kepatuhan terhadap UU PDP sebelum masa retensi berakhir, fasyankes berisiko melanggar ketentuan administrasi kesehatan dan kehilangan alat bukti krusial dalam sengketa medis. Sebaliknya, penolakan terhadap hak subjek data dapat dianggap sebagai pelanggaran hak asasi privasi yang diatur dalam UU PDP. Oleh karena itu, diperlukan aturan pelaksana yang lebih spesifik untuk mengharmonisasikan kedua regulasi ini, misalnya dengan menerapkan mekanisme 'anonymization' (anonimisasi) data di mana identitas pasien dihapus namun data medisnya tetap disimpan untuk kepentingan statistik atau kesehatan publik tanpa melanggar privasi individu.

3. Relevansi UU Kesehatan No. 17 Tahun 2023 dalam Penguatan Eksistensi RME

Keberadaan UU No. 17 Tahun 2023 tentang Kesehatan (Omnibus Law) menghadirkan landasan hukum yang lebih solid dan mutakhir bagi pelaksanaan Rekam Medis Elektronik (RME) di Indonesia. Signifikansi utama undang-undang tersebut tercermin dalam pengakuan secara formal bahwa setiap pasien memiliki hak atas privasi data kesehatannya yang bersifat pribadi, yang wajib dijaga oleh seluruh tenaga medis, tenaga kesehatan, serta pimpinan fasilitas pelayanan kesehatan (Fasyankes). Pasal 286 UU Kesehatan menegaskan bahwa rahasia kesehatan pasien meliputi seluruh data dan informasi terkait kondisi kesehatan pasien yang diperoleh tenaga medis dan tenaga kesehatan selama proses pelayanan kesehatan. Dalam ranah digital, hal ini mengartikan bahwa kewajiban menjaga kerahasiaan tidak lagi hanya menjadi tanggung jawab individual profesi, melainkan berkembang menjadi tanggung jawab bersama institusi dalam mengelola sistem informasi kesehatan yang terlindungi dari akses pihak yang tidak berwenang.

Selain itu, UU Kesehatan No. 17 Tahun 2023 melakukan penyelarasan yang fundamental terhadap aspek digitalisasi melalui pengaturan Sistem Informasi Kesehatan

yang terintegrasi. Pasal 339 mewajibkan setiap Fasyankes untuk menyelenggarakan sistem informasi kesehatan yang mampu beroperasi secara lintas sektor, yang menjadi dasar hukum bagi penerapan RME dalam platform nasional (seperti SATUSEHAT). Kendati demikian, undang-undang ini juga menetapkan pembatasan yang ketat terkait pembukaan rahasia kesehatan; rahasia tersebut hanya dapat dibuka untuk kepentingan kesehatan pasien, pemenuhan permintaan aparat penegak hukum, atau kepentingan publik lainnya sebagaimana diatur dalam undang-undang. Dengan demikian, UU Kesehatan berperan sebagai "benteng yuridis" yang menjamin bahwa meskipun data medis bersifat dinamis dan dapat dipertukarkan demi efisiensi layanan, prinsip kerahasiaan dan privasi tetap menjadi prioritas utama yang tidak dapat dikorbankan dengan alasan teknis semata.

4. Standar Penyelenggaraan Sistem Elektronik dalam Kerangka UU ITE dan PP PSTE

Relevansi perlindungan data medis dalam penyelenggaraan Rekam Medis Elektronik (RME) sangat dipengaruhi oleh posisi fasilitas pelayanan kesehatan (fasyankes) sebagai Penyelenggara Sistem Elektronik (PSE) sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-Undang Nomor 1 Tahun 2024 serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Berdasarkan Pasal 3 PP PSTE, setiap PSE, baik yang bersifat publik maupun privat, wajib menyelenggarakan sistem elektronik yang andal, aman, serta bertanggung jawab atas operasional sistem tersebut sebagaimana mestinya.

Dalam konteks RME, ketentuan ini menimbulkan tanggung jawab hukum bagi fasyankes tidak hanya untuk menyediakan sarana digital bagi pelayanan pasien, tetapi juga untuk memastikan terpenuhinya prinsip ketersediaan (availability), keutuhan (integrity), dan kerahasiaan (confidentiality) data medis dari potensi gangguan teknis maupun ancaman siber.

Selanjutnya, Pasal 15 UU ITE menegaskan bahwa PSE memikul tanggung jawab atas penyelenggaraan sistem elektroniknya. Apabila terjadi kegagalan sistem yang berdampak pada kebocoran data medis, fasyankes dapat dikenai tanggung jawab perdata maupun sanksi administratif apabila terbukti lalai dalam menerapkan standar keamanan yang layak. Ketentuan dalam PP PSTE juga menekankan kewajiban PSE untuk mengelola rekam jejak elektronik (log audit) atas seluruh aktivitas pemrosesan data pribadi. Kewajiban ini menjadi sangat penting dalam proses pembuktian apabila terjadi insiden keamanan siber, karena fasyankes harus mampu menunjukkan identitas pihak yang mengakses data, waktu akses, serta tujuan penggunaannya. Dengan demikian, harmonisasi antara regulasi di bidang kesehatan dan standar PSE dalam UU ITE membentuk sistem perlindungan hukum yang berlapis, di mana keamanan teknologi informasi menjadi prasyarat fundamental bagi keabsahan penyelenggaraan layanan kesehatan digital di Indonesia.

Dalam konteks penegakan hukum, efektivitas Rekam Medis Elektronik (RME) sebagai alat bukti sangat bergantung pada keautentikan rekam jejak elektronik atau log audit. Agar tidak mudah disanggah di persidangan, pengelolaan log audit oleh fasilitas pelayanan kesehatan (fasyankes) sebagai Penyelenggara Sistem Elektronik (PSE) harus memenuhi prinsip integritas dan nirsangkal (non-repudiation) sesuai mandat UU ITE dan PP PSTE. Hal ini berarti setiap aktivitas akses, perubahan, maupun penghapusan data harus tercatat secara otomatis dengan stempel waktu (trusted timestamping) yang sinkron dan tidak dapat dimanipulasi oleh administrator internal sekalipun. Fasyankes wajib menerapkan kontrol akses yang ketat (seperti otentikasi dua faktor) agar identitas subjek hukum yang mengakses data terpeta secara unik dalam log tersebut. Tanpa sistem pengelolaan log yang terenkripsi dan terisolasi dari akses publik, validitas rekam medis sebagai alat bukti elektronik akan mudah digugurkan karena dianggap gagal menjamin

bahwa informasi yang ditampilkan adalah informasi yang sama saat data tersebut pertama kali dibuat.

5. Tata Kelola Data di Platform SATUSEHAT (Kemenkes)

Integrasi Rekam Medis Elektronik (RME) ke dalam platform nasional SATUSEHAT merupakan tonggak sentralisasi data kesehatan di Indonesia yang diinisiasi oleh Kementerian Kesehatan. Secara yuridis, tata kelola dalam platform ini menciptakan struktur akuntabilitas baru di mana tanggung jawab perlindungan data pribadi tidak lagi bersifat terlokalisasi pada satu fasilitas pelayanan kesehatan (fasyankes),Melainkan menjadi tanggung jawab bersama dalam suatu ekosistem digital nasional. Transformasi ini mengharuskan adanya kejelasan mengenai batasan wewenang antara fasyankes selaku pengendali data asal dengan Kementerian Kesehatan selaku pengelola sistem pusat. Sinkronisasi ini menjadi krusial untuk memastikan bahwa pemindahan data dari server lokal menuju basis data nasional tetap berada dalam koridor perlindungan privasi yang konsisten dan tidak melanggar hak-hak subjek data.

Namun, di sisi lain, pengumpulan data medis berskala masif dalam satu platform terpusat secara signifikan meningkatkan profil risiko terhadap serangan siber. SATUSEHAT secara teknis menjadi titik kritis (single point of failure) yang memerlukan protokol keamanan tingkat tinggi guna mencegah terjadinya kebocoran data massal yang dapat melumpuhkan kepercayaan publik terhadap sistem kesehatan digital. Oleh karena itu, tata kelola data di platform ini wajib mengedepankan prinsip transparansi dan kontrol subjek data melalui fitur manajemen persetujuan (consent management). Hal ini bertujuan agar pasien tetap memiliki kedaulatan atas informasi medisnya, sekaligus memastikan bahwa pemanfaatan data kesehatan nasional untuk kepentingan riset atau kebijakan publik tetap berjalan selaras dengan mandat Undang-Undang Pelindungan Data Pribadi (UU PDP).

Oleh karena itu, tata kelola SATUSEHAT harus mengonstruksikan perlindungan hukum yang mampu meredam kecemasan psikologis tersebut melalui transparansi radikal dan penguatan hak kedaulatan data. Secara yuridis, hal ini harus diwujudkan dalam fitur consent management yang memberikan hak eksklusif kepada pasien untuk memberikan atau menarik persetujuan akses bagi pihak tertentu secara real-time. Tanpa adanya jaminan hukum yang memberikan kontrol psikologis kembali kepada pasien, sentralisasi data hanya akan dipandang sebagai ancaman privasi daripada sebuah kemajuan layanan. Perlindungan hukum yang ideal tidak hanya fokus pada ketahanan teknis dari peretasan, tetapi juga pada pemulihan kepercayaan publik melalui regulasi yang memastikan bahwa data dalam SATUSEHAT tidak akan disalahgunakan untuk kepentingan di luar pelayanan kesehatan, seperti diskriminasi asuransi atau keperluan penegakan hukum tanpa prosedur yang ketat.

B. Tantangan Yuridis dan Teknis di Tengah Ancaman Siber

Implementasi Rekam Medis Elektronik (RME) di Indonesia saat ini berada di persimpangan antara efisiensi layanan dan kerentanan keamanan yang signifikan. Secara teknis, tantangan terbesar muncul dari eskalasi serangan siber yang kian canggih, terutama melalui skema ransomware dan advanced persistent threats (APT) yang secara spesifik menyasar sektor kesehatan karena nilai komoditas data medis yang sangat tinggi di pasar gelap. Fasyankes sering kali menjadi titik lemah akibat kesenjangan infrastruktur teknologi informasi, di mana banyak institusi kesehatan belum menerapkan standar enkripsi end-to-end yang memadai serta sistem deteksi intrusi yang mampu bekerja secara real-time. Selain faktor eksternal, kerentanan teknis juga diperparah oleh faktor kelalaian manusia (human error) dan minimnya literasi digital di kalangan tenaga medis, yang sering kali menjadi pintu masuk utama bagi serangan phishing untuk menembus kredensial sistem informasi rumah sakit.

Dari perspektif yuridis, tantangan yang dihadapi tidak kalah kompleks, terutama terkait dengan kejelasan mekanisme pertanggungjawaban hukum saat terjadi kegagalan pelindungan

data. Meskipun UU PDP telah mengatur sanksi, terdapat "kekosongan operasional" mengenai standar minimum teknologi keamanan yang wajib dipenuhi oleh fasyankes dengan skala ekonomi kecil, seperti klinik atau puskesmas, sehingga menciptakan standar perlindungan yang timpang. Selain itu, sifat serangan siber yang sering kali lintas batas negara (borderless) menimbulkan kendala dalam yurisdiksi penegakan hukum pidana siber dan pembuktian digital yang rumit. Di sisi lain, mekanisme tuntutan ganti rugi bagi pasien selaku subjek data masih menghadapi hambatan dalam pembuktian kerugian imateriil dan hubungan kausalitas antara kegagalan sistem dengan kerugian yang dialami pasien. Tantangan-tantangan ini menunjukkan bahwa perlindungan hukum RME saat ini masih bersifat reaktif dan membutuhkan penguatan pada regulasi teknis yang lebih bersifat mandatori dan preventif.

Tantangan substansial dalam penegakan hukum perdata terkait kebocoran data medis di Indonesia terletak pada sulitnya pembuktian kerugian imateriil, terutama pada data bersifat sensitif seperti riwayat HIV/AIDS atau kondisi kesehatan mental. Meskipun UU PDP telah mengklasifikasikan data kesehatan sebagai data spesifik yang kebocorannya dapat berdampak permanen pada harkat dan martabat pasien, hukum perdata Indonesia melalui Pasal 1365 KUHPerdata masih menitikberatkan pada bukti kerugian riil yang bersifat materiil atau dapat dinilai dengan uang. Dalam praktiknya, pasien selaku subjek data seringkali kesulitan mengonversi dampak psikologis, stigmatisasi sosial, atau diskriminasi yang mereka alami menjadi nilai nominal ganti rugi yang terukur secara hukum. Sulitnya membuktikan hubungan kausalitas (causal verband) antara kegagalan sistem keamanan fasyankes dengan dampak traumatis yang bersifat laten ini seringkali membuat posisi tawar pasien menjadi lemah di hadapan pengadilan. Oleh karena itu, diperlukan pergeseran beban pembuktian atau penerapan standar penilaian ganti rugi imateriil yang lebih progresif guna menjamin bahwa hak privasi pasien yang dilindungi konstitusi tidak hanya menjadi slogan normatif tanpa pemulihan hak yang nyata.

C. Konstruksi Perlindungan Hukum yang Ideal dan Preventif dalam Ekosistem RME

Upaya penguatan perlindungan data medis di Indonesia melalui UU PDP dan Permenkes No. 24 Tahun 2022 sebenarnya telah mengadopsi prinsip-prinsip global, namun masih terdapat ruang penyempurnaan jika dibandingkan dengan standar internasional seperti General Data Protection Regulation (GDPR) di Uni Eropa atau Health Insurance Portability and Accountability Act (HIPAA) di Amerika Serikat. GDPR menetapkan standar 'notifikasi kebocoran' yang sangat ketat, di mana pengendali data wajib melaporkan pelanggaran data dalam waktu maksimal 72 jam kepada otoritas pengawas. Sementara itu, HIPAA di Amerika Serikat mewajibkan standar teknis spesifik berupa 'Technical Safeguards yang mencakup enkripsi tingkat lanjut dan access control yang sangat rigid bagi seluruh entitas kesehatan tanpa terkecuali. Di Indonesia, meskipun UU PDP telah menetapkan status data kesehatan sebagai data spesifik dengan standar perlindungan tinggi (golden standard), detail teknis mengenai kewajiban notifikasi dan audit keamanan periodik bagi fasyankes skala kecil masih bersifat umum. Mengadopsi mekanisme Security Rule dari HIPAA dapat menjadi referensi bagi regulator di Indonesia untuk merumuskan standar teknis yang lebih mandatori dan terperinci guna meminimalisir celah eksploitasi siber pada sistem RME.

Membangun sistem perlindungan data medis yang resilien memerlukan pergeseranparadigma hukum dari pendekatan reaktif menuju konstruksi hukum yang bersifat preventif dan teknosentris. Konstruksi perlindungan hukum yang ideal harus mengintegrasikan prinsip Privacy by Design dan Privacy by Default ke dalam setiap regulasi teknis penyelenggaraan Rekam Medis Elektronik (RME). Hal ini berarti perlindungan privasi bukan lagi sekadar kewajiban administratif yang dipenuhi di akhir, melainkan harus menjadi bagian integral dari arsitektur sistem sejak tahap pengembangan awal. Secara yuridis, pemerintah perlu menetapkan standar minimum keamanan informasi yang mandatori dan spesifik bagi tiap tingkatan fasyankes, sehingga terdapat kepastian hukum mengenai parameter enkripsi, otentikasi dua faktor, dan prosedur pemulihan data pasca-insiden yang wajib dipenuhi sebagai syarat izin operasional.

Selain penguatan pada aspek teknis, konstruksi hukum yang ideal juga harus mencakup penguatan fungsi pengawasan melalui lembaga otoritas pelindungan data pribadi yang

independen. Otoritas ini berperan krusial dalam melakukan audit keamanan informasi secara periodik dan memberikan sanksi yang memberikan efek jera, sekaligus menyediakan mekanisme penyelesaian sengketa yang aksesibel bagi pasien. Dari sisi tanggung jawab perdata, perlu dipertimbangkan penerapan doktrin tanggung jawab mutlak (strict liability) atau setidaknya beban pembuktian terbalik bagi fasyankes dalam kasus kebocoran data. Dengan konstruksi ini, pasien tidak lagi dibebankan untuk membuktikan kesalahan teknis sistem yang kompleks, melainkan fasyankeslah yang wajib membuktikan bahwa mereka telah menerapkan standar keamanan maksimal. Pendekatan holistik yang mengombinasikan regulasi yang rigid dengan kepatuhan teknologi yang dinamis inilah yang akan menjamin kerahasiaan medis pasien tetap terlindungi di tengah ancaman siber yang terus berevolusi.

Dalam ekosistem Rekam Medis Elektronik (RME), konstruksi hukum tidak boleh hanya berhenti pada relasi antara pasien dan fasilitas pelayanan kesehatan (fasyankes), tetapi juga harus menjangkau penyedia jasa teknologi atau vendor pihak ketiga. Mengingat banyak fasyankes menggunakan sistem informasi yang dikembangkan oleh pihak eksternal, maka tanggung jawab perlindungan data menjadi tanggung jawab renteng yang harus dituangkan dalam kontrak kerja sama yang memenuhi standar UU PDP. Regulasi ideal harus mewajibkan adanya klausul perlindungan data yang ketat dalam setiap Service Level Agreement (SLA), di mana vendor wajib menjamin bahwa sistem yang mereka bangun memiliki fitur keamanan mutakhir seperti enkripsi end-to-end dan sistem deteksi intrusi otomatis. Ketidakjelasan batasan akses vendor saat ini merupakan celah yuridis yang dapat mengaburkan subjek hukum yang bertanggung jawab saat terjadi kebocoran data di sisi peladen (server) atau aplikasi.

Selanjutnya, efektivitas perlindungan hukum sangat bergantung pada kewajiban pelaksanaan audit keamanan informasi secara berkala yang bersifat mandatori. Implementasi RME di RSU menunjukkan bahwa meskipun protokol dasar seperti penggunaan user ID dan firewall sudah diterapkan, hambatan seperti jarangnya penggantian kata sandi dan penggunaan fitur autofill tetap menjadi ancaman nyata. Oleh karena itu, hukum positif Indonesia perlu mendorong transformasi dari sekadar kepatuhan dokumen (paper compliance) menjadi kepatuhan substantif melalui pemeriksaan teknis yang rutin oleh otoritas independen atau BSSN. Hal ini krusial untuk memastikan bahwa integritas (integrity) dan ketersediaan (availability) data medis tetap terjaga selama masa retensi 25 tahun sebagaimana diamanatkan oleh Permenkes No. 24 Tahun 2022. Tanpa mekanisme audit yang ketat, transformasi digital kesehatan berisiko menjadi sekadar perpindahan media penyimpanan tanpa peningkatan standar keamanan yang berarti.

KESIMPULAN

Penelitian ini menunjukkan bahwa integrasi Rekam Medis Elektronik (RME) dalam ekosistem SATUSEHAT telah didukung oleh kerangka regulasi yang relatif komprehensif, mulai dari UU No. 17 Tahun 2023 tentang Kesehatan, UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, hingga Permenkes No. 24 Tahun 2022 dan regulasi terkait sistem elektronik. Secara normatif, regulasi tersebut telah memberikan landasan yang kuat dalam menjamin kerahasiaan data medis sebagai bagian dari hak asasi manusia, sekaligus menetapkan kewajiban hukum bagi fasilitas pelayanan kesehatan sebagai pengendali data pribadi. Namun demikian, penelitian ini menemukan bahwa masih terdapat tantangan signifikan baik dari aspek yuridis maupun teknis, seperti disharmonisasi norma terkait retensi dan penghapusan data, belum adanya standar teknis keamanan yang bersifat operasional dan mandatori, serta kerentanan terhadap serangan siber yang diperparah oleh faktor internal seperti rendahnya literasi digital dan lemahnya implementasi protokol keamanan. Selain itu, validitas rekam medis elektronik sebagai alat bukti hukum juga masih menghadapi tantangan dalam hal integritas sistem dan pengelolaan log audit.

Keterbatasan penelitian ini terletak pada pendekatan yang digunakan, yaitu yuridis normatif yang berfokus pada analisis regulasi dan literatur tanpa didukung oleh data empiris yang luas dari berbagai fasilitas pelayanan kesehatan. Studi kasus yang digunakan juga masih terbatas pada satu institusi, sehingga belum sepenuhnya merepresentasikan kondisi implementasi RME secara nasional. Di samping itu, penelitian ini belum mengkaji secara mendalam aspek teknis keamanan siber dari sudut pandang teknologi informasi secara praktis.

Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan pendekatan empiris dengan melibatkan lebih banyak sampel fasilitas kesehatan guna memperoleh gambaran yang lebih komprehensif mengenai implementasi RME di Indonesia. Penelitian mendatang juga perlu mengintegrasikan analisis multidisipliner antara hukum, teknologi informasi, dan manajemen risiko untuk merumuskan model perlindungan data medis yang lebih aplikatif. Selain itu, kajian lebih lanjut terkait efektivitas penerapan standar keamanan internasional seperti GDPR dan HIPAA dalam konteks hukum Indonesia menjadi penting guna memperkuat konstruksi regulasi nasional yang adaptif terhadap perkembangan ancaman siber.

DAFTAR PUSTAKA

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas, 113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

ENISA. (2022). *ENISA threat landscape for the health sector*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Greenleaf, G. (2020). Global data privacy laws 2020: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report, 163*, 10–13.

Information Commissioner's Office (ICO). (2021). *What is special category data?* https://ico.org.uk

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Laporan tahunan keamanan siber Indonesia*. Kominfo.

Kementerian Kesehatan Republik Indonesia. (2022). *Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis*.

Kementerian Kesehatan Republik Indonesia. (2023). *Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan*.

Kshetri, N. (2021). Cybersecurity in healthcare: Challenges and opportunities. *IT Professional, 23*(2), 14–18. https://doi.org/10.1109/MITP.2020.3048000

Kruse, C. S., Stein, A., Thomas, H., & Kaur, H. (2018). The use of electronic health records to support population health: A systematic review of the literature. *Journal of Medical Systems, 42*(11), 214. https://doi.org/10.1007/s10916-018-1075-6

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1–10. https://doi.org/10.3233/THC-161263

Mantelero, A. (2013). The future of consumer data protection in the EU: Re-thinking the "notice and consent" paradigm. *Computer Law & Security Review, 30*(6), 643–660. https://doi.org/10.1016/j.clsr.2014.09.001

Suhartono, S. (2023). Implementasi perlindungan data pribadi dalam sistem informasi kesehatan di Indonesia. *Jurnal Hukum dan Teknologi Informasi, 5*(2), 123–135.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

World Health Organization. (2021). *Global strategy on digital health 2020–2025*. WHO. https://www.who.int