Al-Tamimi Kesmas
Jurnal Ilmu Kesehatan Masyarakat (*Journal of Public Health Sciences*)
Volume 15, Nomor 1, Juni 2026, Halaman 39-51
p-ISSN: 2338-2147, e-ISSN: 2654-6485
https://jurnal.ikta.ac.id/index.php/kesmas

PERLINDUNGAN HUKUM TERHADAP KEAMANAN DATA REKAM MEDIS ELEKTRONIK PASIEN

Indra Narendra[1]✉, Albertha Yulia Pratiwi[2], Darsono[3], Widia Rahmatullah[4]
[(1,2,3)]D3 Rekam Medis dan Informasi Kesehatan, Politeknik Kesehatan Bhakti Setya Indonesia, , Yogyakarta, Indonesia
[(4)]D3 Teknologi Bank Darah, Politeknik Kesehatan Bhakti Setya Indonesia, , Yogyakarta, Indonesia

ARTICLE INFO

Artikel history :

Submitted : 2026-06-04
Accepted : 2026-06-18
Publish : 2026-06-30

Kata kunci :
Perlindungan_hukum; keamanan_data; rekam_medis_elektronik; pasien

ABSTRAK

Klinik sebagai fasilitas pelayanan kesehatan memiliki tanggung jawab dalam memberikan perlindungan hukum terhadap keamanan data pasien yang termuat didalam rekam medis elektronik. Prinsip keamanan tidak jarang terabaikan pada penyelenggaraan rekam medis elektronik di fasilitas pelayanan kesehatan**.** Penelitian ini bertujuan untuk menganalisis perlindungan hukum terhadap prinsip keamanan data rekam medis elektronik pasien terkait dengan aspek kerahasiaan, integritas, dan ketersediaan di Klinik S. Metode yang diterapkan dalam penelitian ini adalah pendekatan deskriptif kualitatif. Hasil penelitian mengindikasikan bahwa Klinik S telah berupaya memberikan perlindungan hukum keamanan data pasien pada aspek kerahasiaan (confidentiality) dengan menerapkan akses sistem dilakukan melalui penggunaan username dan password serta didukung oleh fitur automatic logout. Meskipun demikian, terdapat kelemahan berupa penyimpanan password secara otomatis pada browser sehingga dapat diketahui pihak lain dan belum adanya praktik penggantian password secara rutin oleh tenaga kesehatan. Perlindungan hukum pada aspek integritas (integrity) terdapat fitur edit dan hapus untuk pengguna, meskipun fitur tersebut telah tersedia, masih terdapat kekurangan berupa tidak adanya mekanisme verifikasi dari tenaga kesehatan maupun pihak yang berwenang terhadap setiap perubahan yang dilakukan. Sistem juga memungkinkan perubahan dilakukan kapan saja tanpa pengaturan batas waktu. Perlindungan hukum pada aspek ketersediaan (availability), rekam medis elektronik hanya dapat diakses di dalam lingkungan Klinik S dan dapat diakses diwaktu yang sama (realtime) untuk mendukung kelancaran proses pelayanan kesehatan pada pasien. Perlindungan hukum atas keamanan data pasien sudah diupayakan, namun belum sepenuhnya optimal. Berdasarkan kajian yuridis perlindungan hukum atas keamanan data pasien rekam medis pasien secara preventif maupun represif juga telah diatur berlandaskan kepada peraturan perundang-undangan yang berlaku.

Keywords:
Legal protection; data_security; electronic_medical_record; patient

ABSTRACT

Clinics as health service facilities have the responsibility to provide legal protection for the security of patient data contained in electronic medical records. The principle of security is often neglected in the implementation of electronic medical records in health care facilities. This researche aims to analyze the legal protection of the principle of security of patients electronic medical record data related to the aspects of confidentiality, integrity, and availability in Klinik S. The method applied in this researche is a qualitative descriptive. The results of the researche indicate that Klinik S has made efforts to provide legal protection for patient data security in the aspect of confidentiality by implementing system access through the use of usernames and passwords and supported by the automatic logout feature. However, there are drawbacks in the form of automatic password storage in the browser so that other parties can be known and there is no practice of changing passwords regularly by health workers. Legal protection in the aspect of integrity there is an edit and delete feature for users, even though this feature is available, there are still shortcomings in the form of no verification mechanism from health workers and authorities for every change made. The system also allows changes to be made at any time without setting a time limit. Legal protection in terms of availability, electronic medical records can only be accessed within the S Clinic environment and can be accessed at the same time (realtime) to support the smooth process of health services to patients. Legal protection for patient data security has been sought, but it is not fully optimal. Based on the juridical research of legal protection of patient data security and patient medical records in a preventive and repressive manner, it has also been regulated based on applicable laws and regulations.

✉***Corresponding Author:***

Indra Narendra
Politeknik Kesehatan Bhakti Setya Indonesia, Yogyakarta, Indonesia
Telp. 081315626820
Email: indranarendra@poltekkes-bsi.ac.id

PENDAHULUAN

Klinik adalah fasilitas pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan meliputi pelayanan kesehatan primer dan/atau pelayanan kesehatan lanjutan secara komprehensif spesialistik (Permenkes no 11, 2025). Mutu pelayanan kesehatan di klinik senantiasa perlu ditingkatkan dari waktu ke waktu, pengelolaan catatan dan data informasi pasien sudah mengalami transformasi yang sebelumnya menggunakan metode konvensional, saat ini sudah beralih dengan menggunakan elektronik. Pencatatan data pelayanan kesehatan pasien saat ini sudah dikelola melalui sistem informasi kesehatan berupa rekam medis elektronik.

Implementasi rekam medis elektronik disatu sisi memberikan berbagai manfaat, yang diantaranya meningkatkan efisiensi pelayanan, kemudahan akses informasi kesehatan, serta meningkatkan kualitas pengambilan keputusan klinis. Transformasi atas pelaksanaan rekam medis elektronik juga menimbulkan tantangan baru terhadap keamanan data didalamnya berupa meningkatnya risiko kebocoran data informasi, penyalahgunaan akses, manipulasi informasi, serta gangguan terhadap ketersediaan data pasien.

Kasus serangan *ransomware wannacry* pada 2017 yang melumpuhkan layanan *National Health Service* (NHS) Inggris dan menyebabkan kerugian hingga £92 juta menegaskan rapuhnya infrastruktur kesehatan terhadap serangan siber ditingkat global (Amallia et al., 2025). Peristiwa lain juga pernah terjadi kasus kebocoran data kesehatan menyebabkan informasi rekam medis sekitar enam juta pasien COVID-19 dapat diakses dan tersebar di internet. Data yang terdampak meliputi 48 GB data terkompresi serta 157 GB data tidak terkompresi dengan total 3.250.144.777 data. Informasi yang bocor dalam format CSV mencakup data identitas dan data kesehatan pasien, seperti nama, alamat email, NIK, nomor telepon, ID perangkat, status COVID-19, riwayat pemeriksaan, riwayat pelacakan kontak, dan data vaksinasi (Devi, 2025). Kebocoran data kesehatan merupakan permasalahan yang serius karena keterbukaan informasi medis pribadi dapat meningkatkan risiko penyalahgunaan data, termasuk pencurian identitas, penipuan finansial, serta dampak psikologis yang merugikan bagi pemilik data (Nadiroh & Wiraguna, 2025).

Perlindungan atas keamanan data perlu dipahami dengan baik sebelum menerapkan rekam medis elektronik. *Health Insurance Portability Accountability-Act* menyatakan ada tiga pilar yang direkomendasikan untuk memastikan bahwa informasi kesehatan yang dilindungi tetap aman, yaitu dengan penerapan pengamanan administratif, pengamanan fisik, dan pengamanan teknis (Keshta & Odeh, 2021). Prinsip-prinsip keamanan informasi kesehatan pasien pada rekam medis elektronik juga perlu memperhatikan aspek *privacy, confidentiality, integrity, availability, non-repudiation, authentication, dan authorization* (Tiorentap & Hosizah, 2020). Berdasarkan regulasi hukum tentang rekam medis menyatakan bahwa penyelenggaraan rekam medis elektronik harus menjamin keamanan data melalui penerapan tiga aspek utama, yaitu kerahasiaan, integritas, dan ketersediaan informasi (Permenkes RI No 24, 2022).

Aspek kerahasiaan merupakan jaminan atas keamanan data dan informasi dari gangguan pihak internal maupun eksternal yang tidak memiliki hak akses, sehingga data dan informasi yang ada dalam rekam medis elektronik terlindungi penggunaan dan penyebarannya (Permenkes RI No 24, 2022). Kerahasiaan rekam medis elektronik harus senantiasa dijaga oleh seluruh pihak di fasilitas pelayanan kesehatan. Perlindungan atas kerahasiaan (*confidentiality*) data pasien pada sistem rekam medis elektronik dapat diwujudkan melalui penerapan kontrol keamanan, antara lain autentikasi pengguna

dengan *username dan password*, penghentian sesi secara otomatis (*automatic logout*), penggunaan teknologi kriptografi untuk melindungi data, serta pembatasan akses melalui sistem keamanan jaringan (Sofia et al., 2022).

Aspek integritas (*integrity*) merupakan jaminan terhadap keakuratan data dan informasi yang ada dalam rekam medis elektronik, perubahan terhadap data hanya boleh dilakukan oleh orang yang diberi hak akses, sehingga data yang ada dalam rekam medis elektronik terlindungi dari kesalahan pengisian maupun pemalsuan (Permenkes RI No 24, 2022). Prinsip keamanan data rekam medis elektronik pasien pada aspek integritas (*integrity*) difasilitas pelayanan kesehatan dapat menerapkan sistem perubahan data, *audit trail*, validator secara khusus yang ditunjuk, riwayat perubahan yang dapat terlacak waktu, bagian yang dirubah dan dapat mendeteksi pengguna yang melakukan perubahan.

Aspek ketersediaan (*availability*) merupakan jaminan data dan informasi yang ada dalam rekam medis elektronik dapat tersedia jika dibutuhkan dan diakses serta digunakan oleh orang yang telah memiliki kewenangan (Permenkes RI No 24, 2022). Rekam medis elektronik harus bisa memastikan bahwa sistem dan data pasien dapat diakses oleh tenaga kesehatan yang berwenang kapan pun diperlukan untuk perawatan pasien, terutama dalam situasi darurat, penerapannya dapat dilakukan dengan sistem cadangan dan rencana pemulihan bencana atau biasa dikenal dengan sistem *back up*. Aspek ketersediaan (*availability*) adalah aspek yang menekankan pada tersedianya informasi saat diakses oleh pihak pihak yang terkait. Sebagai alat komunikasi, rekam medis harus selalu dapat diakses dengan cepat dan dapat menampilkan kembali data yang telah tersimpan sebelumnya (Suhariyono et al., 2025).

Negara wajib menjamin hak-hak hukum warga negaranya, perlindungan hukum merupakan pengakuan terhadap harkat dan martabat warga negaranya sebagai manusia (Utomo et al., 2020). Perlindungan hukum memberikan pengayoman terhadap hak asasi manusia (HAM) yang dirugikan orang lain dan perlindungan itu diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh hukum (Rahardjo, 2021). Menurut Philpus M Hadjon sebagaimana dikutip didalam jurnal sulilopu menyatakan, perlindungan hukum terhadap masyarakat dapat diwujudkan melalui dua bentuk, yaitu preventif dan represif. Perlindungan preventif berfungsi sebagai langkah pencegahan terhadap potensi sengketa dengan mengarahkan pemerintah agar lebih hati-hati dalam menggunakan diskresi saat mengambil keputusan. Sementara perlindungan represif berperan dalam penyelesaian sengketa yang telah terjadi, termasuk melalui proses di lembaga peradilan (Sulolipu et al., 2019).

Perlindungan keamanan data rekam medis elektronik pasien juga merupakan bagian dari perlindungan hukum atas hak privasi dan hak atas keamanan data pribadi sebagaimana dijamin dalam sistem hukum di Indonesia. Keberadaan perlindungan hukum yang efektif merupakan aspek fundamental dalam mendukung kepercayaan masyarakat terhadap penggunaan rekam medis elektronik. Implementasinya memerlukan penguatan regulasi yang berlaku, peningkatan kapasitas infrastruktur keamanan teknologi informasi, serta penyelenggaraan edukasi yang berkesinambungan bagi tenaga kesehatan dan masyarakat umum.

Penelitian terdahulu masih memiliki keterbatasan karena umumnya berorientasi pada aspek teknis keamanan data rekam medis elektronik dan belum banyak mengkaji dari perspektif perlindungan hukum keamanan data rekam medis elektronik pasien, selain itu, penelitian yang membahas dan mengintegrasikan keamanan data rekam medis elektronik pasien atas aspek kerahasiaan (*confidentiality)*, integritas (*integrity*), dan ketersediaan (*availability*) dengan bentuk perlindungan hukum preventif dan represif

pada fasilitas pelayanan kesehatan tingkat pertama, khususnya klinik, masih terbatas. Dengan demikian, mengindikasikan belum optimalnya kajian yang menganalisis implementasi keamanan data rekam medis elektronik pasien berdasarkan kerangka kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*)-(CIA) sekaligus meninjau implikasinya terhadap perlindungan hukum pasien.

Penelitian ini menggunakan kerangka keamanan data rekam medis elektronik pasien sebagai dasar evaluasi penyelenggaraan rekam medis elektronik yang dikaitkan secara langsung dengan konsep perlindungan hukum pasien dalam pelayanan kesehatan. Penelitian ini tidak hanya mengidentifikasi penerapan keamanan data rekam medis elektronik pasien, tetapi juga menganalisis konsekuensi hukum sebagai salah satu bentuk perlindungan hukum yang dapat diberikan kepada pasien apabila terjadi pelanggaran keamanan data rekam medis elektronik.

Klinik S dipilih sebagai lokasi penelitian karena telah menerapkan rekam medis elektronik dalam proses pelayanan pasien sejak tahun 2019. Klinik S belum memiliki tenaga kesehatan yang berprofesi sebagai perekam medis dan informasi kesehatan, rekam medis elektronik di Klinik S dikelola oleh tenaga kesehatan lain yang secara kompetensi kurang mendalami dan memahami pengelolaan keamanan data rekam medis elektronik pasien. Sistem yang dirancang oleh Klinik S bertujuan untuk mempermudah pengelolaan rekam medis pasien secara digital dan menggantikan penggunaan arsip medis manual yang saat ini kurang efisien. Penggunaan rekam medis elektronik juga memiliki tantangan tersendiri bagi Klinik S terutama terkait dengan keamanan data yang termuat didalamnya. Tidak terlindunginya keamanan data rekam medis elektronik pasien memiliki konsekuensi hukum.

Berdasarkan studi pendahuluan di Klinik S, setiap tenaga kesehatan dan non kesehatan yang berwenang memiliki *username* dan *password* masing-masing untuk mengakses rekam medis elektronik, namun dalam penerapannya *username* dan *password* kurang terjaga kerahasiaannya seorang tenaga kesehatan yang satu dapat mengetahui *username* dan *password* rekan kerja lainnya. Diperoleh fakta adanya satu peristiwa ketika seorang tenaga kesehatan menggunakan akun rekannya dan salah menginput data sosial pasien, secara sistem akan membaca kesalahan input mengarah kepada *username* dan *password* yang digunakan, meskipun pelakunya belum tentu pemilik *username* dan *password* yang sebenarnya. Temuan ini merupakan kesenjangan empiris yang menjadi dasar didalam penelitian ini. Pihak manajemen perlu segera mengambil suatu tindakan agar tidak mengancam keamanan data pasien serta mencegah pelanggaran terhadap keamanan data rekam medis elektronik pasien.

Berdasarkan uraian pada bagian pendahuluan ini, pentingnya klinik dalam menjaga keamanan data rekam medis elektronik pasien guna memberikan perlindungan hukum bagi pasien didalam pelayanan kesehatan atas data pribadi yang disampaikan. Tujuan dari penelitian ini adalah Menganalisis perlindungan hukum yang dikaitkan dengan aspek kerahasiaan (*Confidentiality*), aspek integritas (*Integrity*), aspek ketersediaan (*Availability*).

METODE

Jenis Penelitian

Penelitian ini menerapkan pendekatan deskriptif kualitatif yang bertujuan untuk memberikan gambaran secara sistematis mengenai fenomena yang diteliti, baik yang terjadi secara alami maupun yang berkaitan dengan aktivitas manusia. Hasil penelitian difokuskan pada deskripsi dan analisis objek penelitian tanpa dimaksudkan untuk

menghasilkan generalisasi atau implikasi yang bersifat universal. Penelitian kualitatif adalah metodologi penelitian yang digunakan untuk meneliti kondisi objek alamiah, dimana peneliti sebagai *instrument* kunci (Sugiyono, 2020).

Rancangan penelitian yang diterapkan adalah studi kasus, yaitu metode yang digunakan untuk menelaah suatu permasalahan secara mendalam melalui pengkajian terhadap satu atau lebih kasus. analisis mencakup pengkajian terhadap karakteristik kasus, peristiwa yang berkaitan dengan kasus tersebut, serta respons dan tindakan yang muncul sebagai konsekuensi dari perlakuan atau eksposur tertentu yang dialami subjek penelitian. (Notoatmodjo, 2018).

Lokasi dan Waktu Penelitian

Tempat penelitian berada di Klinik S, Sleman, Yogyakarta, Waktu penelitian ini dilaksanakan pada Desember 2024 – Maret 2025.

Populasi dan Subjek Penelitian

Populasi dalam penelitian ini berjumlah 36 orang, teknik pengambilan sampel dilakukan dengan cara non probability dengan pendekatan teknik purposive sampling dengan jumlah sampel berjumlah 7. Subjek penelitian ini terdiri dari seluruh tenaga kesehatan dan non kesehatan yang menggunakan rekam medis elektronik di Klinik S. Kriteria sampel ditentukan dengan cara mengambil satu dari masing-masing profesi dari anggota populasi tanpa ada pengecualian, dengan kategori petugas yang telah bekerja selama minimal 2 tahun. Pemilihan masa kerja minimal 2 tahun dilakukan untuk memastikan bahwa subjek penelitian memiliki pengalaman yang memadai dalam menggunakan sistem rekam medis elektronik, sehingga dapat memberikan data yang relevan untuk penelitian ini.

Tehnik Pengumpulan Data

Teknik pengambilan data menggunakan cara wawancara terstruktur, observasi, dan studi dokumentasi, instrumen penelitian berupa pedoman wawancara, alat perekam, pedoman checklist observasi, dan pedoman studi dokumentasi. Analisis data dalam penelitian kualitatif, dilakukan pada saat pengumpulan data berlangsung, dan setelah selesai pengumpulan data dalam periode tertentu (Sugiyono, 2020).

Definisi Operasional

Definisi operasional yang digunakan dalam penelitian ini adalah sebagai berikut; Perlindungan hukum bertujuan memastikan bahwa data rekam medis elektronik pasien memperoleh jaminan keamanan yang sah sesuai dengan ketentuan peraturan perundang-undangan, dan upaya yang dilakukan dalam memberikan perlindungan data. Aspek kerahasiaan adalah memastikan bahwa data rekam medis elektronik terlindungi kerahasiaannya dan hanya diakses oleh pihak yang memiliki kewenangan. Aspek integritas (Integrity) adalah memastikan keakuratan data dan menjamin bahwa perubahan data informasi rekam medis elektronik dapat terdeteksi riwayatnya, dan dapat dilakukan oleh otoritas yang berwenang. Aspek ketersediaan adalah memastikan bahwa informasi dan data yang termuat pada rekam medis elektronik senantiasa bisa terakses oleh pengguna yang berwenang saat dibutuhkan dalam pelayanan kesehatan, serta upaya dengan *backup* data untuk memastikan dapat dipulihkan.

Analisis Data

Proses analisis data dilakukan melalui tahapan reduksi data, penyajian data, dan penarikan kesimpulan. Reduksi data dilakukan dengan menyeleksi, memfokuskan, dan merangkum informasi yang sesuai dengan tujuan penelitian sehingga data menjadi lebih terorganisasi dan mudah dipahami. Data yang telah direduksi kemudian disajikan dalam bentuk uraian naratif serta penjelasan terhadap gambar berdasarkan hasil pengumpulan

data. Penarikan kesimpulan dilakukan dengan menyajikan hasil dari temuan data yang telah dianalisis dan mengambil kesimpulan secara umum. Keabsahan data dilakukan melalui uji validitas dengan menggunakan teknik triangulasi.
Dalam penelitian ini, triangulasi sumber ditetapkan untuk memastikan validitas data dengan cara membandingkan informasi yang diperoleh dari beberapa sumber yang berbeda.

HASIL

1. Menganalisis perlindungan hukum prinsip keamanan data rekam medis elektronik pasien berdasarkan aspek kerahasiaan (*confidentiality*)

Aspek kerahasiaan (*confidentiality*) merupakan salah satu prinsip keamanan data rekam medis elektronik yang bertujuan menjaga data pasien dari akses yang tidak sah dan menjamin bahwa rekam medis elektronik hanya dapat diakses oleh pihak yang berwenang. Rekam medis elektronik yang digunakan di Klinik S telah menggunakan sistem *login* sehingga mengharuskan tenaga kesehatan memasukkan *username* dan *password*, hal tersebut menunjukan bahwa Klinik S telah mengimplementasikan langkah awal pengamanan data untuk menjaga aspek kerahasiaan setiapkali menggunakan rekam medis elektronik.

Gambar 1 Tampilan Menu *Login*

Berdasarkan pengambilan data melalui wawancara dengan responden, Klinik S berupaya menjaga keamanan data rekam medis elektronik dengan cara akses terhadap rekam medis elektronik harus dilakukan menggunakan *username* dan *password* yang dimiliki secara khusus oleh masing-masing tenaga kesehatan. Kerahasiaan kredensial tersebut perlu dijaga agar setiap tindakan yang dilakukan dalam sistem dapat diidentifikasi serta dapat dipertanggungjawabkan oleh pengguna yang bersangkutan. Responden memahami bahwa *username* dan *password* bersifat rahasia dan tidak mengetahui *username* dan *password* milik rekan kerja lainnya, namun terdapat responden yang menyampaikan bahwa masih ada tenaga kesehatan yang saling mengetahui *username* dan *password* rekan kerjanya.

Username dan *password* yang diketahui antar tenaga kesehatan/rekan kerja mengindikasikan kurang optimalnya aspek kerahasiaan rekam medis elektronik. Data maupun keterangan yang telah diperoleh, selanjutnya dilakukan uji keabsahan dengan triangulasi sumber yang menyatakan upaya menjaga keamanan data rekam medis elektronik pasien pada aspek kerahasiaan (*confidentiality*) yaitu setiap tenaga kesehatan yang mengakses rekam medis elektronik harus mempunyai *username* dan *password* masing-masing dan merahasiakannya, namun dalam praktiknya *username* dan *password* tenaga kesehatan dapat tersimpan secara otomatis di *browser Chrome*, sehingga memungkinkan tenaga kesehatan atau rekan kerja lainnya dapat saling mengetahui. Klinik S juga telah menetapkan karakteristik tertentu dalam pembuatan *username* dan *password* oleh tenaga kesehatan. Pergantian *password* secara berkala juga diperlukan sebagai tindakan pencegahan akses oleh pihak yang tidak berkepentingan. Meskipun

demikian, hasil wawancara dengan responden menunjukkan bahwa tenaga kesehatan belum secara konsisten melakukan pembaruan *password* sesuai periode yang ditetapkan.

Perlindungan hukum atas jaminan keamanan data rekam medis elektronik pasien pada aspek kerahasiaan lainnya, Klinik S telah meggunakan fitur *automatic logout.* Fitur ini dinilai penting karena mampu secara otomatis mengeluarkan pengguna dari rekam medis elektronik apabila tidak terdapat aktivitas dalam kurun waktu tertentu sehingga dapat mencegah terjadinya akses oleh pihak yang tidak berwenang, terutama ketika pengguna lupa melakukan *logout* atau meninggalkan perangkat dalam kondisi masih aktif.

Terdapat perbedaan pernyataan dari responden mengenai keberadaan fitur *automatic logout* pada sistem rekam medis elektronik di Klinik S, terdapat responden menyatakan bahwa sistem dapat secara otomatis melakukan *logout* jika tidak ada aktivitas dalam beberapa menit. Triangulasi sumber menyatakan untuk fitur otomatis *logout* sudah ada penerapannya selama kurang lebih 10 menit dari aktifitas terakhir pada rekam medis elektroniknya.

2. Menganalisis perlindungan hukum prinsip keamanan data rekam medis elektronik pasien berdasarkan aspek integritas (*integrity*)

Aspek integritas atau *integrity* yaitu menjamin keakuratan data dan memastikan bahwa perubahan informasi pada rekam medis elektronik tetap terjaga keamanannya. Keakuratan dan perubahan data harus bisa dilakukan dan dapat diketahui riwayatnya, data informasi rekam medis elektronik tidak dapat diubah tanpa persetujuan dari otoritas pihak yang berwenang. Rekam medis elektronik di Klinik S terdapat fitur edit dan hapus ketika diperlukan untuk melakukan perubahan data.

Gambar 2. Fitur Perubahan Data

Berdasarkan hasil wawancara dengan responden di Klinik S, menunjukkan bahwa sistem sudah memiliki fitur edit dan hapus, sistem juga dapat mencatat waktu dan tanggal perubahan, namun nama akun atau identitas pengguna yang melakukan perubahan tidak terekam dan tidak terlacak riwayatnya.

Terdapat responden yang tidak mengetahui mengenai riwayat perubahan seperti waktu, tanggal, dan nama akun dapat tercatat atau tidaknya didalam perubahan rekam medis elektronik, ada juga responden yang menyatakan belum pernah menggunakan fitur

tersebut secara langsung. Triangulasi sumber menyatakan dalam rangka memberikan perlindungan hukum atas keamanan data rekam medis elektronik pasien dalam aspek integritas (*integrity*) di Klinik S sudah terdapat fitur pengeditan, dan penghapusan, dan perubahan yang dilakukan dapat diketahui riwayat waktu, tanggal perubahannya, namun untuk melacak nama akun yang melakukan perubahan belum dapat dilakukan.

Berdasarkan wawancara dengan responden menyatakan perubahan dan penghapusan data rekam medis elektronik di Klinik S dapat dilakukan oleh tenaga kesehatan dengan melakukan akses langsung tanpa harus melalui konfirmasi atau persetujuan dari pihak lain yang memiliki kewenangan khusus. Tanpa adanya verifikasi dari pihak yang berwenang, perubahan data dapat dilakukan secara langsung tanpa pengecekan atau persetujuan, hal ini menunjukkan bahwa belum terdapat mekanisme pembatasan akses atau kontrol. Pembatasan kewenangan dilakukan dengan cara**,** tenaga kesehatan yang bertugas pada bagian pendaftaran hanya memiliki akses untuk mengedit atau menghapus data pada tahap pendaftaran pasien, dan tidak memiliki kewenangan untuk mengubah data klinis yang dicatat oleh dokter, perawat, atau tenaga medis lainnya.

Perubahan data atas rekam medis elektronik di Klinik S juga belum menerapkan batasan waktu, tenaga kesehatan masih dapat mengedit data tanpa adanya pembatasan waktu tertentu sejak data pertama kali di *entry*. Triangulasi sumber juga menyatakan tidak adanya pembatasan waktu untuk melakukan perubahan atas rekam medis elektronik di Klinik S.

3. Menganalisis perlindungan hukum prinsip keamanan data rekam medis elektronik pasien pada aspek ketersediaan (*Availability*)

Aspek ketersediaan (*availability*) adalah prinsip yang memastikan data rekam medis elektronik tetap dapat diakses dan digunakan oleh pihak yang berwenang setiap kali dibutuhkan untuk mendukung pelayanan kesehatan. Berdasarkan hasil pengambilan data melalui wawancara dengan responden diketahui rekam medis elektronik dapat diakses secara langsung, ketika saat berada di jangkauan Klinik S, untuk diluar klinik maka rekam medis elektronik tidak dapat diakses. Responden juga menginformasikan rekam medis elektronik senantiasa tersedia dan dapat diakses secara instan ketika diperlukan oleh tenaga kesehatan, sehingga mendukung kelancaran proses pelayanan kesehatan secara langsung di Klinik S.

Perlindungan hukum atas keamanan data rekam medis elektronik pasien pada aspek integritas juga diupayakan melalui mekanisme *backup* data, penerapan *cloud backup* manual pada Klinik S dapat memberikan jaminan bahwa data penting terlindungi. Sistem *backup* yang diterapkan memastikan data tetap dapat dipulihkan jika terjadi gangguan pada sistem utama, sehingga kelangsungan operasional Klinik berjalan. Triangulasi sumber juga menyatakan untuk memberikan jaminan perlindungan hukum atas ketersediaan data, rekam medis elektronik hanya bisa diakses dilingkungan wilayah Klinik saja, dan untuk menjamin adanya ketersediaan data ketika terjadi *eror* ataupun *downsystem* Klinik S sudah memiliki mekanisme pencadangan data (*Backup data).*

Perlindungan hukum atas keamanan data rekam medis elektronik dalam penelitian ini juga ditunjang dengan adanya hasil observasi atas penerapan keamanan data rekam medis elektronik pasien sebagai berikut :

Tabel 1 hasil observasi atas penerapan keamanan data rekam medis elektronik pasien

Aspek Kerahasiaan yang diamati	Hasil Ya	Hasil Tidak	Keterangan
Akses rekam medis elektronik menggunakan *username* dan *password*	√		Ya, RME di Klinik Pratama S sudah menggunakan *username* dan *password* pada tampilan awal untuk mengakses kedalamnya.
Terdapat *automatic logout* jika rekam medis elektronik tidak digunakan	√		Ya *automatic logout* sudah ada pada sistem rekam medis elektonik di Klinik Pratama S dengan penerapan 10 menit.
Rekam medis elektronik memungkinkan pengeditan dan penghapusan data rekam medis pasien	√		Ya, RME di Klinik S bisa melakukan pengeditan dan penghapusan.
Rekam medis elektronik secara otomatis menyimpan riwayat perubahan (*history*) setiap kali data rekam medis diedit atau dihapus dan tertera informasi mengenai waktu, tanggal perubahan, dan nama akun.	√		Ya, langsung terganti yang terbaru, dan jika di edit tercatat waktu dan tanggal, namun nama akun yang melakukan perubahan tidak ada.
Mekanisme backup data untuk menghindari kehilangan informasi penting.	√		Ya, menggunakan sistem *cloud backup* manual.

PEMBAHASAN

Aspek kerahasiaan (*confidentiality*) adalah prinsip keamanan yang memastikan bahwa data dan informasi rekam medis elektronik hanya dapat diakses oleh pihak yang berwenang, sehingga terlindungi dari gangguan atau penyalahgunaan oleh pihak yang tidak memiliki otorisasi, sehingga data dan informasi akan terlindungi penggunaan dan penyebarannya. Perlindungan hukum atas keamanan data rekam medis elektronik pasien pada asepek kerahasiaan di Klinik S telah menerapkan sistem *login* yang mengharuskan setiap tenaga kesehatan untuk memasukan *username* dan *password*, hal ini sebagaimana dengan hasil penelitian terdahulu yang menyatakan pengguna sebelum masuk ke dalam sistem informasi perlu mengetik atau memasukkan *username* beserta *password* (Sofia et al., 2022).

Upaya menjaga keamanan data rekam medis elektronik pasien pada aspek kerahasiaan lainnya dilakukan dengan mengubah *password* secara berkala setiap dua hingga tiga bulan, namun tenaga kesehatan di Klinik S belum menerapkan penggantian *password* secara berkala. Pergantian *password* yang tidak dilakukan secara berkala di Klinik S, mencerminkan adanya kelemahan dalam menjaga keamanan data pasien dalam aspek kerahasiaan dan tidak sesuai dengan penelitian terdahulu yang menekankan pentingnya pembaruan *username* dan *password* secara berkala sebagai langkah pengamanan terhadap kemungkinan akses oleh pihak yang tidak bertanggung jawab, hal ini disebabkan data akses pengguna dapat diketahui oleh petugas lain sehingga membuka peluang terjadinya akses tanpa otorisasi (Wardani et al., 2024). Keberhasilan dalam mengimplementasikan perlindungan hukum atas kerahasiaan data rekam medis

elektronik tidak hanya ditentukan oleh regulasi yang ditetapkan dan keandalan sistem teknologi informasi yang digunakan. Perilaku pengguna dalam mengakses dan memanfaatkannya juga ikut andil dalam menjaga keamanan data rekam medis elektronik pasien (James, 2021). Pelatihan keamanan data bagi tenaga kesehatan perlu dirancang tidak sekadar untuk meningkatkan pengetahuan pengguna tentang keamanan siber, tetapi juga untuk membentuk perilaku yang mendukung perlindungan keamanan data dengan cara memerangi pelanggaran maupun penyimpangan yang dipengaruhi manusia seperti tidak menjaga kerahasiaan *username* dan *password* dari pihak lain, maupun tidak melakukan perggantian secara berkala.

Klinik S menerapkan fitur *automatic logout* yang secara otomatis keluar dari sistem setelah tidak ada aktivitas selama 10 menit, hal ini sebagaimana penelitian terdahulu yang menyatakan mekanisme tersebut berperan penting dalam mengurangi risiko akses tidak sah, terutama saat pengguna meninggalkan sistem tanpa menutup atau keluar dari akun yang sedang aktif (Suhariyono et al., 2025). Keberadaan fitur *automatic logout* di Klinik S berfungsi sebagai mekanisme pengamanan tambahan yang secara otomatis mengakhiri sesi pengguna setelah periode tidak aktif tertentu. Penerapan fitur ini penting untuk mengurangi risiko penggunaan sistem oleh pihak yang tidak memiliki hak akses, terutama ketika pengguna meninggalkan perangkat tanpa melakukan *logout* terlebih dahulu.

Adanya fitur *logout* otomatis di Klinik S, sejalan dengan penelitan sebelumnya bahwa fitur otomatis *logout* dapat mengantisipasi orang yang tidak berhak menggunakan sistem informasi tersebut, jika pengguna meninggalkan komputer dalam waktu relatif lama (Sofia et al., 2022).

Secara yuridis perlindungan hukum atas keamanan data rekam medis elektronik pasien pada aspek kerahasiaan diatur berdasarkan peraturan perundang-undangan yang berlaku. Setiap orang berhak memperoleh perlakuan yang adil, mendapatkan pelayanan kesehatan yang bermutu, aman, dan sesuai dengan kebutuhan (Undang-Undang, No 17, 2023). Hak atas kerahasiaan data dan informasi kesehatan pribadi merupakan bagian penting dari perlindungan hukum atas keamanan data rekam medis elektronik pasien dalam sistem pelayanan kesehatan.

Penyelenggara sistem elektronik berkewajiban untuk menjaga dan melindungi data pribadi yang dimiliki oleh pengguna, termasuk keamanan data rekam medis elektronik pasien. Apabila prinsip kerahasiaan ini dilanggar maka perlindungan hukum secara represif ditegakkan dengan dikenakan sanksi pidana**.** Berdasarkan pasal 27 ayat 1 jo pasal 45 ayat 1 undang-undang informasi transaksi elektronik menyebutkan bahwa "Setiap Orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum" dapat dikenakan sanksi dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah) (Undang-Undang No 1, 2024).

Integritas (*Integrity*) merupakan jaminan terhadap keakuratan data dan informasi yang ada dalam Rekam Medis Elektronik, dan perubahan terhadap data hanya boleh dilakukan oleh orang yang diberi hak akses untuk mengubah (Permenkes RI No 24, 2022). *Integrity* merupakan aspek yang berkaitan dengan perubahan informasi, segala bentuk perubahan yang dilakukan pada sistem atau rekam medik elektronik, dapat diketahui oleh sistem yang ada. Pembetulan kesalahan pada rekam medis konvensional hanya dapat dilakukan dengan cara pencoretan tanpa menghilangkan catatan yang dibetulkan dan dibubuhi paraf dokter, dokter gigi atau tenaga kesehatan tertentu yang

bersangkutan. Pencoretan tentu saja tidak bisa dilakukan pada rekam medis elektronik, oleh karenanya diperlukan pengamanan atau proteksi lebih yaitu segala bentuk perubahan maupun penghapusan dapat dilacak dan diketahui riwayatnya (Sofia et al., 2022).

Rekam Medis Elektronik di Klinik S sudah ada fitur edit dan hapus, dimana data informasi yang diubah akan langsung tergantikan dengan informasi terbaru. Sistem juga mencatat waktu dan tanggal perubahan, namun nama akun atau identitas pengguna yang melakukan perubahan tidak terekam dalam sistem. Perubahan data dapat dilakukan tanpa ada pembatasan waktu dan dapat dilakukan sesuai dengan kebutuhan, hal ini tidak sejalan dengan pengaturan penyelenggaraan rekam medis. Perbaikan data dapat dilakukan apabila terjadi kesalahan dalam penginputan data administratif dan data klinis pasien dan hanya dapat dilakukan oleh tenaga kesehatan pemberi pelayanan kesehatan dan petugas administrasi termasuk perekam medis dan informasi kesehatan dengan batas waktu paling lama 2x24 jam sejak data diinput (Permenkes RI No 24, 2022). Tenaga kesehatan di Klinik S memiliki akses langsung untuk melakukan perubahan atau penghapusan data informasi pasien tanpa perlu melalui konfirmasi atau persetujuan dari pihak lain yang bertanggung jawab. Tanpa adanya verifikasi dari tenaga kesehatan atau petugas yang berwenang, perubahan data dapat dilakukan secara langsung tanpa proses pengecekan, yang berpotensi mengganggu integritas data medis pasien.

Secara yuridis perlindungan hukum atas keamanan data rekam medis elektronik pasien pada aspek integritas (*integrity*) diatur berdasarkan peraturan perundang-undangan yang berlaku. Pengendali data wajib menjamin keakuratan, keutuhan, data pribadi, termasuk data medis elektronik. Apabila integritas data tidak dijaga, seperti membiarkan akses bebas tanpa pencatatan yang jelas atas perubahan data**,** maka dapat dianggap sebagai pelanggaran terhadap prinsip perlindungan data pribadi, dalam hal pengendali data tidak dapat menjaga keamanan data rekam medis elektronik pasien pada asepek integritas dapat dikenai sanksi administratif**,** seperti teguran tertulis, denda administratif, hingga penghentian sementara aktivitas pengolahan data (Undang-Undang No 27, 2022). Berdasarkan pasal 32 ayat 1 undang-undang informasi dan transaksi elektronik menyatakan bahwa Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, atau menyembunyikan Informasi atau Dokumen Elektronik milik orang lain atau publik. Pengaturan lebih lanjut atas sanksi pelanggaran terhadap perubahan data tanpa hak dapat diancam pidana penjara 8 Tahun dan atau denda paling banyak 2.000.000.000 (dua miliar rupiah) (Undang-Undang No 1, 2024).

Ketersediaan (a*vailabilit**y***) merupakan jaminan data dan informasi yang ada dalam rekam medis elektronik dapat diakses dan digunakan oleh orang yang telah memiliki hak akses yang ditetapkan oleh pimpinan fasilitas pelayanan kesehatan (Permenkes RI No 24, 2022). Penyelenggaraan rekam medis elektronik di Klinik S senantiasa dapat tersedia pada saat dibutuhkan ketika pelayanan kesehatan berlangsung. Data yang terdapat pada rekam medis elektronik dapat diakses secara *real-time* oleh tenaga kesehatan saat pelayanan kesehatan dilakukan di dalam klinik, sehingga mendukung kelancaran proses pelayanan medis secara langsung. Perlindungan hukum atas keamanan data rekam medis elektronik pasien pada aspek ketersediaan telah dilengkapi dengan sistem *cloud backup manual*.

Penerapan tersebut memberikan jaminan ketersediaan data walau terjadi gangguan pada server utama ataupun jaringan, hal ini sejalan dengan penelitian sebelumnya yang menyatakan penyelenggaraan sistem elektronik wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum, yaitu mampu menampilkan kembali informasi

elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang diterapkan dalam peraturan perundang-undangan (Sofia et al., 2022). Apabila aspek ketersediaan tidak terpenuhi, seperti tidak tersedianya data saat dibutuhkan untuk tindakan medis atau tidak adanya sistem pemulihan data saat gangguan, maka hal ini dapat dianggap sebagai bentuk kelalaian. Kegagalan dalam menjamin ketersediaan data dapat berdampak pada keselamatan pasien dan memunculkan tanggung jawab hukum.

Secara yuridis, perlindungan hukum terhadap keamanan data rekam medis elektronik pasien pada aspek ketersediaan (*availability*) telah diatur dalam peraturan perundang-undangan yang berlaku. Ketentuan tersebut tercantum dalam Pasal 26 ayat (1) peraturan mengenai penyelenggaraan sistem dan transaksi elektronik yang menyatakan bahwa setiap penyelenggara sistem elektronik wajib menjamin kerahasiaan, keutuhan, keautentikan, keteraksesan, ketersediaan, serta keterlacakan informasi elektronik dan/atau dokumen elektronik sesuai dengan ketentuan hukum yang berlaku.

Perlindungan hukum secara represif atau berupa penindakan dapat dilakukan, pelanggaran terhadap ketentuan yang berlaku dapat mengakibatkan dikenakannya sanksi administratif berupa teguran tertulis, denda administratif, penghentian sementara kegiatan pengolahan data, hingga pencabutan izin penyelenggaraan sistem elektronik (Peraturan pemerintah No 71, 2019).

SIMPULAN

Perlindungan hukum atas keamanan data rekam medis elektronik pasien di Klinik S sudah diupayakan dengan meninjau beberapa aspek penting. Aspek kerahasiaan (*confidentiality*), masih belum optimal karena tidak dilakukan pergantian *username* dan *password* secara berkala. Aspek integritas (*Integrity*) belum sepenuhnya terjaga keamanan datanya. Rekam medis elektronik belum dapat melacak riwayat perubahan yang dilakukan secara keseluruhan, dan belum diterapkannya batas waktu perbaikan data 2x24 jam. Aspek ketersediaan (*Availability*) sudah optimal, data rekam medis elektronik dapat diakses secara *real-time* oleh tenaga kesehatan dan mendukung kelancaran proses. Perlindungan hukum secara preventif dalam kajian yuridis dapat diketahui dengan adanya pengaturan-pengaturan yang mewajibkan klinik untuk menjaga keamanan data. Perlindungan hukum secara represif dilakukan dengan adanya penerapan sanksi hukum baik pidana, perdata, dan administrasi negara atas pelanggaran keamanan data rekam medis elektronik pasien.

DAFTAR PUSTAKA

Amallia, S., Happy Putra, D., Agung Satrya, B., & Rosmala Dewi, D. (2025). Strategi Pengamanan Data Sistem Informasi Kesehatan: Studi Literatur Kasus Kebocoran dan Upaya Keamanan Global. *Prosiding Seminar Nasional Rekam Medis Dan Infromasi Kesehatan 2025*, *1*, 113–208.

Devi, N. M. (2025). *Dugaan Kebocoran Data Aplikasi PeduliLindungi: Publik Resah, Pemerintah Diminta Perkuat Keamanan Siber*. Kompasiana. https://www.kompasiana.com/najwamustika14/691d1df134777c322e33ec62/dugaan-kebocoran-data-aplikasi-pedulilindungi-publik-resah-pemerintah-diminta-perkuat-keamanan-siber

James, L. (2021). *Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis By Liu Hua Yeo, MS, and James Banfield, PhD*.

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Nadiroh, A., & Wiraguna, S. A. (2025). Analisis Yuridis Kebocoran Data di Layanan Kesehatan Digital: Studi Kasus Aplikasi Telemedicine di Indonesia. *Media Hukum Indonesia (MHI)*, *2*(6), 313–320. https://doi.org/10.5281/zenodo.15520536

Notoatmodjo. (2018). *Metodologi Penelitian Kesehatan*. PT. Rineka.

Peraturan pemerintah No 71. (2019). Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik. In *Media Hukum* (Vol. 7, Issue 2).

PERMENKES RI NO 11, 2025. (2025). *PERMENKES RI NO 11 Tahun 2025*.

Permenkes RI No 24. (2022). Permenkes RI No 24 Tahun 2022 Tentang Rekam Medis. *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022*, *151*(2), 10–17.

Rahardjo, S. (2021). *Ilmu Hukum* (cetakan 9). PT. Citra Aditya Bakti.

Sofia, S., Ardianto, E. T., Muna, N., & Sabran, S. (2022). Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, *1*(2), 94–103. https://doi.org/10.47134/rmik.v1i2.29

Sugiyono. (2020). *Metodologi Penelitian Kuantitatif, Kualitatif dan R & D*.

Suhariyono, U. S., Rusdian Ikawati, F., & Afifah, N. (2025). Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso. *Jurnal Manajemen Informasi Kesehatan Indonesia*, *13*(1), 2337–2585. https://jmiki.aptirmik.or.id/jmiki/article/view/812/367

Sulolipu, A. B., Handoyo, S., & Roziqin. (2019). Perlindungan Hukum Terhadap Profesi Dokter Dalam Penyelesaian Sengketa Medis Berdasarkan Prinsip Keadilan Legal Protection of the Professional Doctor in the Settlement of Medical Disputes Based on the Principle of Justice. *Jurnal Projudice : Jurnal Online Mahasiswa Pascasarjana Uniba*, *1*(1), 60–82. http://jurnal.pascasarjana.uniba-bpn.ac.id/index.php/JurnalProjudice/article/view/29

Tiorentap, H. (2020). Aspek Keamanan Informasi Dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check Up MP. *Predicting the Next President*, *November*, 197–202. https://doi.org/10.5040/9798216426998.ch-013

Undang-Undang, 17. (2023). Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 Tentang Kesehatan. In *Undang-Undang* (Issue 187315).

Undang-Undang No 1. (2024). *Undang-Undang RI Nomor 1 Tahun 2024* (Vol. 44, Issue 8).

Undang-Undang No 27, I. (2022). Perlindungan Data Pribadi. In *Republik Indonesia*.

Utomo, H. P., Gultom, E., & Afriana, A. (2020). Urgensi Perlindungan Hukum Data Pribadi Pasien Dalam Pelayanan Kesehatan Berbasis Teknologi Di Indonesia. *Jurnal Ilmiah Galuh Justisi*, *8*(2), 168. https://doi.org/10.25157/justisi.v8i2.3479

Wardani, E., Putra, D. H., Sonia, D., & Yulia, N. (2024). Keamanan Sistem Informasi Rekam Medis Elektronik di Rumah Sakit Islam Jakarta Sukapura. *RAMMIK: Jurnal Rekam Medik Dan Manajemen Informasi Kesehatan*, *3*(2), 31–38. https://rammik.pubmedia.id/index.php/rmik/article/view/1756/21