



Evaluasi Aspek Keamanan dan Kerahasiaan Rekam Medis Elektronik (RME) Berdasarkan *Cyber Security* di Rumah Sakit Jiwa Dr. Soeharto Heerdjan

Ferlia Sintiana Dewi^{1*}, Bangga Agung Satrya², Nanda Aula Rumana³, Laela Indawati⁴, Nurhidayatulloh⁵

¹⁻⁴Program Studi Rekam Medis dan Informasi Kesehatan, Universitas Esa Unggul, Indonesia

⁵Rumah Sakit Jiwa DR. Soeharto Heerdjan, Indonesia

Email: ferliasintiana23@student.esaunggul.ac.id¹, bangga.agung@esaunggul.ac.id², nanda.rumana@esaunggul.ac.id³, laela.indawati@esaunggul.ac.id⁴, nurhidayat2174@gmail.com⁵

*Penulis Korespondensi: ferliasintiana23@student.esaunggul.ac.id

Abstract. Hospitals implementing Electronic Medical Records (EMR) must ensure patient data security and confidentiality based on cybersecurity principles to prevent data breaches and misuse. EMR at Dr. Soeharto Heerdjan Mental Hospital has been implemented since 2019, but security issues remain, including shared login credentials and low cybersecurity awareness, which may compromise sensitive mental health data. This study aims to describe EMR security and confidentiality based on cybersecurity principles and analyze related threats and risks. A descriptive qualitative method was employed through in-depth interviews, observations, and document analysis involving medical record officers, IT staff, and nurses. Data were analyzed using the Miles and Huberman model. The results show that all seven security and confidentiality aspects have been implemented, but confidentiality, authentication, and non-repudiation remain weak due to simple passwords, shared logins, and the absence of Multi-Factor Authentication (MFA). Cybersecurity measures include firewalls, data encryption, and backup/recovery, although security log monitoring and recovery testing are not routine. The main threat is insider threats, followed by malware, phishing, and network disruptions. Strengthening layered authentication, regular security evaluations, and cybersecurity awareness is recommended.

Keywords: Cyber Threats; Cybersecurity; Data Confidentiality; Data Security; Electronic Medical Records.

Abstrak. Rumah sakit yang menerapkan Rekam Medis Elektronik (RME) wajib menjamin keamanan dan kerahasiaan data pasien berdasarkan prinsip-prinsip keamanan siber (*cybersecurity*) untuk mencegah kebocoran dan penyalahgunaan data. RME di RSJ Dr. Soeharto Heerdjan telah diterapkan sejak 2019, tetapi masih terdapat permasalahan keamanan, termasuk penggunaan kredensial *login* bersama dan rendahnya kesadaran terhadap keamanan siber, yang dapat membahayakan data kesehatan mental pasien yang sensitif. Penelitian ini bertujuan untuk mendeskripsikan keamanan dan kerahasiaan RME berdasarkan prinsip-prinsip keamanan siber serta menganalisis ancaman dan risiko yang terkait. Penelitian ini menggunakan metode kualitatif deskriptif melalui wawancara mendalam, observasi, dan studi dokumentasi yang melibatkan petugas rekam medis, staf IT, dan perawat. Data dianalisis menggunakan model Miles dan Huberman. Hasil penelitian menunjukkan bahwa ketujuh aspek keamanan dan kerahasiaan telah diterapkan, tetapi aspek *confidentiality*, *authentication*, dan *non-repudiation* masih lemah karena penggunaan kata sandi sederhana, *login* bersama, dan belum diterapkannya *Multi-Factor Authentication* (MFA). Upaya keamanan siber meliputi *firewall*, enkripsi data, dan *backup/recovery*, meskipun pemantauan *log* keamanan dan pengujian pemulihan belum dilakukan secara rutin. Ancaman utama adalah *insider threats*, diikuti *malware*, *phishing*, dan gangguan jaringan. Penguatan autentikasi berlapis, evaluasi keamanan secara berkala, dan peningkatan kesadaran keamanan siber direkomendasikan.

Kata kunci : Ancaman Siber; Keamanan Data; Keamanan Siber; Kerahasiaan Data; Rekam Medis Elektronik.

1. LATAR BELAKANG

Seiring dengan perkembangan Teknologi Informasi dan Komunikasi (TIK) serta kemajuan ilmu pengetahuan yang semakin pesat, berbagai dampak dan manfaat dirasakan dalam kehidupan manusia, salah satunya di bidang pelayanan kesehatan yaitu rumah sakit (We'e et al., 2023). Berdasarkan UU No.17 Tahun 2023 menjelaskan bahwa rumah sakit adalah fasilitas pelayanan kesehatan yang menyediakan layanan kesehatan yang lengkap seperti

pelayanan promosi, pencegahan, pengobatan, pemulihan serta paliatif, rumah sakit juga menawarkan layanan rawat inap, rawat jalan, serta penanganan darurat (Republik Indonesia, 2023).

Salah satu perkembangan teknologi tersebut adalah Rekam Medis Elektronik (RME) (Wirajaya & Dewi, 2020). Rekam medis harus diselenggarakan secara elektronik dengan prinsip keamanan dan kerahasiaan data serta informasi (Min-Fang et al., 2019). Dengan disahkannya Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis, seluruh fasilitas pelayanan kesehatan diwajibkan untuk menerapkan RME sesuai dengan standar yang telah ditetapkan oleh kementerian kesehatan (Kemenkes RI, 2022). Penerapan RME di rumah sakit dipercaya dapat meningkatkan kualitas pelayanan dan mencapai tingkat kesehatan masyarakat yang optimal. RME juga dibutuhkan untuk mempermudah akses informasi, perbaikan dokumentasi dan mengurangi kesalahan (Wardani et al., 2024). Namun, penggunaan RME dapat membawa tantangan yang signifikan terutama berkaitan dengan aspek keamanan dan kerahasiaan data pasien (Rani et al., 2024).

Secara keseluruhan, keamanan (*security*), privasi (*privacy*), kerahasiaan (*confidentiality*), dan keselamatan (*safety*) adalah perangkat yang membentengi informasi dalam rekam medis (Hutauruk & Astuti, 2018). Keamanan RME yang dicantumkan dalam Permenkes RI No. 24 Tahun 2022 pada pasal 29 menjelaskan bahwa RME harus memenuhi prinsip keamanan data dan informasi meliputi kerahasiaan, integritas, dan ketersediaan (Kemenkes RI, 2022). Ancaman keamanan *cyber* menjadi semakin krusial seiring dengan pesatnya transformasi digital. Para pelaku kejahatan *cyber* terus mengembangkan berbagai metode baru yang semakin canggih untuk mengancam dan menyerang sistem informasi milik organisasi (Ahmad et al., 2025). Keberhasilan implementasi RME tidak hanya bergantung pada ketersediaan teknologi, tetapi juga pada komitmen institusi kesehatan dalam menyediakan pelatihan, memperkuat kebijakan keamanan informasi, dan meningkatkan kesadaran etika seluruh tenaga medis terhadap pentingnya perlindungan data pasien (Ramadhani et al., 2024).

Berdasarkan penelitian terdahulu terkait analisis implementasi prinsip CIA Triad dalam sistem RME di RSUD X Jawa Tengah, penerapan belum berjalan optimal. Aspek *confidentiality* masih lemah karena penggunaan autentikasi sederhana dan hak akses administrator yang terlalu luas. *Integrity* terganggu akibat mekanisme validasi dan audit *trail* yang belum memadai, sedangkan *availability* cukup baik dengan *uptime* 98,5%, namun masih terkendala gangguan listrik dan jaringan (Setyaningrum & Ricky, 2025). Penelitian sebelumnya di Rumah Sakit AL dr. Mintohardjo menunjukkan bahwa sistem keamanan RME melalui kontrol akses, autentikasi, enkripsi data, *audit trail*, *fingerlock*, *firewall*, antivirus, dan

backup data berhasil menjaga kerahasiaan, integritas, serta ketersediaan informasi pasien. Namun, kelemahan masih terdapat pada kesadaran petugas terhadap keamanan *password*, koneksi internet yang tidak stabil, serta belum adanya prosedur pemulihan data yang hilang (Mahendra et al., 2025). Berdasarkan hasil penelitian di Klinik *Medical Check-Up* Medika Plaza terkait aspek keamanan dalam ISO 27001, hasil *gap analysis* menunjukkan pencapaian keamanan masih rendah, yaitu kerahasiaan 60%, integritas 31%, autentikasi 48%, ketersediaan 25%, kontrol akses 56%, dan *non-repudiation* 33% (Tiorentap & Hosizah, 2020).

Rumah Sakit Jiwa Dr. Soeharto Heerdjan adalah rumah sakit khusus untuk pelayanan kesehatan jiwa kelas A yang terletak di Jalan Prof. Dr. Latumeten No.1, Jakarta Barat. Rumah sakit ini menangani data medis pasien yang sangat sensitif. Rumah sakit ini sudah menerapkan sistem RME sejak tahun 2014 dan disempurnakan pada tahun 2019. Dikarenakan data pasien dengan gangguan jiwa yang sangat sensitif dapat berpotensi kebocoran data di era digital ini, maka penting juga untuk memperkuat aspek keamanan dan kerahasiaan data.

Berdasarkan beberapa penelitian terdahulu yang telah dijelaskan, keterbaruan penelitian ini terletak pada objek dan konteks yang diteliti. Dari ketiga hasil penelitian tersebut belum mengkaji secara khusus terkait aspek keamanan dan kerahasiaan RME pada rumah sakit khusus jiwa. Selain itu, penelitian ini juga tidak hanya menilai aspek teknis sistem keamanan, tetapi juga mengintegrasikan perspektif *cyber security* secara menyeluruh yang mencakup kesiapan kebijakan, kesadaran SDM, serta hambatan teknis dan non teknis.

Berdasarkan hasil observasi awal dan wawancara yang dilakukan kepada kepala rekam medis, petugas rekam medis, dan 2 petugas IT terkait keamanan dan kerahasiaan RME di RSJ Dr. Soeharto Heerdjan menunjukkan bahwa rumah sakit sudah menerapkan RME dalam pelayanannya secara menyeluruh terkecuali pada pelayanan rawat inap yang masih dilakukan secara *hybrid*, tetapi dalam penerapan RME masih ditemukan beberapa kendala dalam prosedur keamanan dan kerahasiaan data pasien, seperti gangguan teknis, penggunaan akses *login* bersama, adanya gangguan jaringan serta hambatan pada SDM yang kurang memahami terkait pentingnya keamanan *cyber* tersebut. Kondisi ini menandakan adanya potensi risiko terhadap kerahasiaan data pasien, sehingga diperlukan penelitian lebih lanjut mengenai aspek keamanan dan kerahasiaan RME terhadap *cyber security* di RSJ Dr. Soeharto Heerdjan.

Berdasarkan latar belakang di atas peneliti tertarik untuk mengetahui permasalahan-permasalahan yang mempengaruhi penerapan aspek keamanan dan kerahasiaan pada RME terhadap *cyber security* di RSJ Dr. Soeharto Heerdjan.

2. KAJIAN TEORITIS

Rumah Sakit

Rumah sakit merupakan institusi pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara paripurna. Berdasarkan UU No.17 Tahun 2023 menjelaskan bahwa Rumah Sakit adalah fasilitas pelayanan kesehatan yang menyediakan layanan kesehatan yang lengkap seperti pelayanan promosi, pencegahan, pengobatan, pemulihan serta paliatif, rumah sakit juga menawarkan layanan rawat inap, rawat jalan, serta penanganan darurat (Republik Indonesia, 2023). Rumah sakit memiliki peran penting sebagai fasilitas pelayanan kesehatan yang harus mampu meningkatkan kualitas pelayanan dan dapat dijangkau oleh masyarakat.

Rekam Medis Elektronik

Dalam Peraturan Menteri Kesehatan Republik Indonesia No.24 Tahun 2022 menjelaskan bahwa Rekam Medis Elektronik adalah jenis rekam medis yang dibuat dengan menggunakan sistem elektronik dan sistem tersebut diperuntukkan bagi penyelenggaraan rekam medis (Kemenkes RI, 2022). RME terdapat dalam sebuah sistem yang secara khusus dirancang untuk mendukung pengguna dengan memberi kemudahan dalam medeteksi kelengkapan dan keakuratan data dengan memberi tanda waspada atau peringatan untuk mendukung keputusan klinis (Suhariyono et al.,2025).

Keamanan dan Kerahasiaan Rekam Medis

Pada haknya setiap pasien mempunyai hak untuk mendapat jaminan keamanan atas data pribadi, yaitu data identitas pasien dan proses pelayanan kesehatan. Penyelenggara pelayanan kesehatan harus mempertimbangkan keamanan dari gangguan yang berasal dari pihak internal maupun eksternal, sehingga data dan informasi yang tersimpan dalam RME tetap terjaga dan terlindungi dari penggunaan serta penyebaran yang tidak sah (Nugroho & Kurniadi, 2022). Informasi tentang pasien adalah rahasia dan rumah sakit diminta untuk menjaga kerahasiaan informasi pasien serta menghormati kebutuhan privasinya. Kerahasiaan merupakan pembatasan pengungkapan informasi pribadi tertentu. Dalam hal ini mencakup tanggung jawab untuk menggunakan, mengungkapkan, atau mengeluarkan informasi hanya dengan sepengetahuan dan izin individu. Kerahasiaan RME mencakup data pribadi pasien serta informasi mengenai layanan kesehatan atau pengobatan yang diberikan kepada pasien.

Cyber Security

Cyber security atau keamanan siber adalah praktik menjaga teknologi dan perangkat lunak komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari akses ilegal atau gangguan. Umumnya, tujuan utama *cyber security* adalah untuk menjaga kerahasiaan,

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif untuk memperoleh pemahaman mendalam mengenai implementasi, tantangan, serta kebijakan keamanan dan kerahasiaan Rekam Medis Elektronik (RME) terhadap *cyber security*. Penelitian dilaksanakan di Rumah Sakit Jiwa Dr. Soeharto Heerdjan, Jakarta Barat, pada November 2025–Juni 2026. Informan penelitian dipilih menggunakan *purposive sampling* dengan jenis *criterion sampling*, yang terdiri atas Kepala Rekam Medis, Petugas Rekam Medis, Petugas IT, dan Perawat, dengan jumlah informan disesuaikan hingga mencapai kejenuhan data. Instrumen penelitian yang digunakan berupa pedoman wawancara dan lembar observasi. Teknik pengumpulan data dilakukan melalui wawancara mendalam (*in-depth interview*), observasi, dan studi dokumentasi terhadap dokumen terkait keamanan data, SOP, kebijakan IT, serta laporan audit keamanan jika tersedia. Data dianalisis secara interaktif menggunakan model Miles dan Huberman yang meliputi reduksi data, penyajian data, serta penarikan kesimpulan dan verifikasi. Keabsahan data dilakukan melalui triangulasi sumber dan triangulasi metode dengan membandingkan hasil wawancara dari setiap informan serta hasil wawancara, observasi, dan studi dokumentasi.

Hasil Penelitian



Berdasarkan hasil analisis pada gambar 1 dapat terlihat bahwa visualisasi data tersebut membentuk suatu jaringan yang saling terhubung antara 6 informan dengan tema-tema utama penelitian. Hasil pengelolaan data pada aplikasi Nvivo menampilkan struktur pengkodean (*coding*) yang terbagi ke dalam tiga tema utama (*parent node*), yaitu penerapan aspek keamanan dan kerahasiaan RME, prinsip-prinsip *cyber security* dan potensi ancaman serta risiko *cyber security* terhadap RME. Kemudian setiap *parent node* terdapat juga *child node* (sub-tema). Pada tema pertama sub temanya ada 6 yaitu SOP & kebijakan keamanan, pengendalian hak akses, kerahasiaan data pasien, pengelolaan data RME, monitoring dan evaluasi serta kendala implementasi yang mempresentasikan praktik operasional dan kebijakan institusi dalam menjaga keamanan RME. Tema kedua sub temanya menjelaskan landasan teori keamanan informasi yaitu CIA *Triad*, *authentication & access control*, keamanan infrastruktur serta *business continuity*. Dan terakhir pada tema ketiga sub temanya ada 5 yaitu ancaman internal, ancaman eksternal, risiko operasional, risiko teknologi dan strategi mitigasi yang menggambarkan identifikasi ancaman serta upaya penanggulangannya.

Keterhubungan antar tema dalam gambar diatas tersebut ditunjukkan melalui dua jenis garis yaitu garis berlabel “*child*” menggambarkan hubungan hierarki antara tema utama dengan sub temanya, sedangkan garis yang berlabel “*codes*” menghubungkan setiap sub tema dengan 6 informan, yaitu kepala rekam medis (P01), petugas rekam medis (P02), petugas IT (PJ keamanan) (P03.1), petugas IT (PJ software) (P03.2), perawat RJ (P04.1) dan terakhir perawat RI (P04.2). Banyaknya garis yang menghubungkan seluruh sub tema dengan lebih dari 1 informan menunjukkan bahwa setiap tema dalam penelitian ini didukung oleh data dari berbagai sumber secara konsisten sehingga memperkuat triangulasi data dan validitas temuan penelitian.

Dengan itu, jaringan yang terbentuk pada gambar 1 menggambarkan secara visual antara 3 tema utama tersebut yang seleuruhnya diperoleh dan diverifikasi melalui hasil wawancara mendalam dengan keenam informan dilingkungan rumah sakit.

Mengidentifikasi Penerapan Aspek Keamanan dan Kerahasiaan RME

Confidentiality (Kerahasiaan)

Aspek kerahasiaan di RSJ Dr. Soeharto Heerdjan diterapkan melalui mekanisme *login* dengan menggunakan *username* dan *password* yang bersifat individual untuk setiap *user*. Setiap petugas memiliki akun yang tidak dapat digunakan bersama sehingga data pasien hanya dapat diakses oleh pihak yang berwenang. Rumah sakit menggunakan enkripsi SHA-256 pada sebagian data yang tersimpan di database. Akses ke sistem RME hanya dapat dilakukan dari

dalam jaringan rumah sakit dengan menggunakan IP publik yang telah di *whitelist*. Temuan diperkuat dengan pernyataan berikut ini :

“enkripsi-nya, kalau gak salah kita pake HT-S256, tapi ini merupakan standar umum buat production. Enkripsi itu ketika data disimpan ke database dari aplikasi itu sudah melakukan enkripsi, jadi saat masuk ke database sebagian data udah dienkripsi, jadi tidak bisa kebaca”-P03.1, Petugas IT (PJ Keamanan)

“disini kan ada PIN masing-masing petugas itu berbeda-beda PIN-nya. Jadi petugas lain tidak bisa akses ke akun kita, maupun sebaliknya. Jadi hanya kita yang bisa lihat. Kemudian setiap selesai menggunakan sistem harus segera di logout agar tidak bisa dibuka oleh orang lain”-P04.2, Perawat RI

Kendala yang ditemukan adalah penggunaan *password* yang masih lemah dan tidak kompleks. Sekitar 20% pengguna masih menggunakan *password* standar tanpa kombinasi huruf besar, angka, dan simbol. Petugas IT juga menemukan beberapa kasus penyimpanan *password* (*autosave password*) di browser komputer bersama sehingga berisiko terhadap kerahasiaan data.

Integrity (Integritas)

Integritas data di RSJ Dr. Soeharto Heerdjan dijaga melalui mekanisme penguncian data setelah 1x24 jam. Setelah melewati batas waktu tersebut, data tidak dapat lagi dimodifikasi tanpa izin khusus dari tim SIMRS. Setiap perubahan data tercatat dalam sistem log, dan hanya pengguna yang menginput data (berdasarkan akun masing-masing) yang dapat memodifikasi data tersebut dalam batas waktu yang ditentukan.

“sekarang kita RME udah dikunci 1x24 jam, jadi itunya ya setiap semua kegiatan harus kelar dalam 1x24 jam, jangan tunda-tunda. Kalau takut lupa atau bagaimana-bagaimana, gitu jadi kekunci”-P01, Kepala Rekam Medis

Validasi data dilakukan secara manual melalui proses verifikasi dua arah, yaitu saat input data pasien baru dan saat pengiriman data ke BPJS atau Satu Sehat, berikut penjelasannya:

“biasanya data tindakan, data hasil kan berhubungan diverif ya untuk BPJS data itu terdetect sama kesesuaian data apakah pasiennya benar atau enggak tindakannya ini itu”-P03.1, Petugas IT (PJ Keamanan)

Beberapa kasus human error berupa kesalahan nama dan nomor rekam medis yang hampir serupa ditemukan oleh P04.2. Namun, hal tersebut dapat ditangani melalui mekanisme double cross check sebelum data tersimpan.

Availability (Ketersediaan)

Ketersediaan sistem RME dijaga melalui penggunaan *server cloud* dengan jaminan uptime 99,99% dari vendor. Sistem backup dilakukan setiap hari pukul 02.00-04.00 WIB secara otomatis. Terdapat server cadangan (*redundancy*) baik pada pihak vendor maupun internal rumah sakit. Target *Recovery Time Objective* (RTO) sistem adalah 30 menit untuk *server cloud* dan maksimal 60 menit untuk pemulihan penuh.

"prosesnya adalah backup data itu tidak bisa melakukan live jadi satu hari sebelumnya yang bisa ke backup itu ada diserver kita server internal, tapi kalau backup mereka yang live itu dicloud mereka juga itu langsung live setiap saat ke server mereka, tapi satu hari yang ke belakang ke backup itu dikita setiap jam 3-4 pagi"-P03.1, Petugas IT (PJ Keamanan)

Gangguan sistem (*downtime*) pernah dialami beberapa kali dengan rata-rata penanganan 5-30 menit. Saat terjadi *downtime*, petugas menggunakan prosedur manual dan menginput kembali data ke sistem setelah sistem pulih.

"Kalau itu satu bulan sekali pasti ada ya, kayak gitu tapi enggak lama gitu. Misalnya, ini kok muter-muter nih, lapor ke SIRS ya langsung ini sih misalnya masalah ya, paling lama 30 menit lah mereka selesai."-P04.1, Perawat RJ

Authentication (Autentikasi)

Autentikasi pengguna di RSJ Dr. Soeharto Heerdjan saat ini menggunakan kombinasi *username* dan *password* dengan kebijakan penggantian *password* setiap 90 hari (3 bulan). Sistem akan secara otomatis meminta pengguna mengganti *password* jika telah melewati batas waktu tersebut. Kebijakan *password* mewajibkan minimal 8 karakter dengan kombinasi *alphanumeric*.

Saat ini sedang dalam proses implementasi biometrik (*fingerprint*) untuk autentikasi saat input CPPT sebagai lapisan keamanan tambahan, namun *Multi-Factor Authentication* (MFA) untuk proses login belum diterapkan. P03.1 menjelaskan rencana pengembangan :

"Rencananya kita tuh mau nerapin menggunakan multi-factor autentikasi. Nah itu menurut mereka adanya yang terbaru dan ini juga penggunaan kombinasi huruf kalau misalnya nggak sesuai masuknya." -P03.1, Petugas IT (PJ Keamanan)

"Sejauh yang saya lihat sih udah cukup aman, tapi untuk presentasinya masih belum aman banget. Masih dikisaran kalau di presentasinya 70%. Karena dari kombinasi passwordnya enggak rumit hanya berupa angka, jadi enggak ada yang spesifik harus ada simbol, harus ada apa."-P04.2, Perawat RI.

Access Control (Kontrol Akses)

Kontrol akses diterapkan melalui *Role-Based Access Control* (RBAC) di mana setiap pengguna mendapatkan hak akses sesuai dengan profesi dan jabatannya. Terdapat pembagian *role* antara dokter, perawat, farmasi, gizi, rekam medis, dan petugas lainnya, masing-masing dengan menu dan hak akses yang berbeda. Akses ke sistem RME hanya dapat dilakukan dari dalam jaringan rumah sakit (pembatasan berdasarkan IP publik), sementara akses dari luar memerlukan VPN dengan permohonan tertulis. Berikut penjelasan mengenai pembagian *role* :

"Kita di sini ada dua akses, eh tiga akses ada dokter, perawat, sama yang nonnakes jadi masing-masing itu beda, beda untuk aksesannya, beda akses menu beda akses inputnya."-P03.2, Petugas IT (PJ Software)

"Langsung dinonaktifkan. Saya lapor ke tim IT, bikin berita acara dengan nama si Anu apa namanya, dengan nomor pegawainnya. Sudah tidak aktif kembali. Sudah tidak akunnya di nonaktifkan."-P01, Kepala Rekam Medis

Authorization (Otorisasi)

Otorisasi di RSJ Dr. Soeharto Heerdjan diimplementasikan melalui pembatasan tindakan yang dapat dilakukan oleh setiap pengguna sesuai dengan role-nya. Hanya pengguna yang membuat data yang dapat mengedit dan menghapus data tersebut. Untuk tindakan penghapusan data oleh pihak di luar pemilik akun harus melalui tim SIMRS dengan disertai alasan yang jelas. Berikut kutipan yang menggambarkan mekanisme otorisasi:

"Kalau untuk kesalahan-kesalahan yang selalu diperbaiki itu penginputan untuk administrasi, room cas hanya yang bisa untuk menghapuskan itu dari SIMRS. Jadi biasanya room cas itu kan per hari dia ada room cas kelas satu 500 hari ini... Kalau bukan bagian kita, kita lapornya ke tim SIRS, minta dihapuskan."-P04.2, Perawat RJ

"Saya admin bisa, tapi nanti di storynya kelihatan. Jadi dia yang buat, dia yang ngapus."-P01, Kepala Rekam Medis

Non-Repudiation (Tidak Dapat Disangkal)

Prinsip *non-repudiation* diterapkan melalui sistem pencatatan aktivitas (*audit trail*) yang merekam setiap tindakan pengguna pada sistem RME. Informasi yang tercatat meliputi *username* pengguna, waktu aktivitas, dan jenis tindakan yang dilakukan (input, edit, hapus). Data *audit trail* disimpan selama rekam medis pasien masih aktif dalam sistem, P03.2 menjelaskan fungsi *audit trail*:

"Wah penting banget karena kalau tanpa itu kita jadinya tunjuk-tunjukkan nuduh-nuduhan tanpa ada bukti kalau misalnya ada audit trail kan apa semuanya kelihatan jadi oh yang saya merasa tidak merubah kok bisa berubah? pas dilihat oh ternyata user ini yang merubah

jadi kan kita ada bukti yang konkret bahwa perubahan itu terjadi atas user ini."-P03.2, Petugas IT (PJ Software)

Namun demikian, *audit trail* hanya ditampilkan pada tampilan admin (super admin) dan tidak terlihat langsung di tampilan pengguna biasa. Pengecekan *audit trail* baru dilakukan jika terjadi masalah atau insiden, dan belum dilaksanakan secara rutin berkala. P01 mengakui hal ini: "Audit trail? Belum ada. Itu yang lagi saya mau bahas sama IT, ya. Kita tuh harusnya ada audit yang misalnya kayak pencatatan atau apa. Belum sampai sana." -P01, Kepala Rekam Medis

Evaluasi Penerapan Prinsip-Prinsip Cyber Security

Firewall dan Intrusion Detection System (IDS)

RSJ Dr. Soeharto Heerdjan telah menerapkan beberapa lapisan keamanan jaringan. Pertama, segmentasi VLAN memisahkan jaringan berdasarkan kategori pengguna (pegawai, tenaga kesehatan, rekam medis, dan pengunjung), sehingga pengunjung tidak dapat mengakses sistem RME. Kedua, *firewall* diterapkan baik di sisi rumah sakit maupun di sisi vendor cloud untuk memfilter akses tidak sah. Ketiga, pembatasan akses berdasarkan IP publik rumah sakit yang telah di-*whitelist*. Dan yang terakhir *endpoint protection (next-generation antivirus)* dipasang di semua *workstation*. Berikut kutipan penjelasan mekanisme keamanan jaringan:

"Pertama membatasi vlan jadi vlan itu dibagi gak hanya satu tapi terpecah sesuai dengan kriterianya dia pegawai, rekam medis, nakes, terus sama pengunjung itu yang pertama, yang kedua firewallnya karna dibatasi karena sudah ada vlan yang membatasi lebih enak lagi di firewall dibatasi si koneksi si staff."-P03.1, Petugas IT (PJ Keamanan). Mekanisme deteksi akses mencurigakan dilakukan secara otomatis melalui *analyzer* pada *firewall* yang memblokir percobaan *brute force*. Namun, sistem *log monitoring* keamanan belum dilakukan secara rutin harian dan hanya diperiksa jika terdapat kejadian yang mencurigakan.

Enkripsi Data

Enkripsi data diterapkan menggunakan algoritma SHA-256 untuk sebagian data yang tersimpan di database. Transmisi data dari klien ke server menggunakan protokol HTTPS yang menjamin keamanan data saat dalam perjalanan (*data in transit*). Namun, enkripsi belum diterapkan secara menyeluruh pada seluruh *field* data di database (baru sebagian data yang dienkripsi). Berikut kutipan penggunaan algoritma enkripsi:

"Pakenya SHA256. Lebih kepada untuk ini kalau misalnya ketika user meng input data semuanya itu transkripsi dengan algoritma jadi untuk data yang di input itu tidak bisa dibaca langsung kecuali memang di inputkan untuk algoritma dan itu memang hanya ada tersedia di aplikasinya saja." P03.2, Petugas IT (PJ Software)

Evaluasi terhadap metode enkripsi yang digunakan belum pernah dilakukan secara formal oleh tim internal RSJ, dan seluruh tanggung jawab enkripsi sepenuhnya berada di pihak vendor “Periksa ID”. Hal ini dikonfirmasi oleh :

"Jujur kita belum pernah melakukan evaluasi tapi kita hanya sebatas yaudah kita nerapkan, ya."-P03.2, Petugas IT (PJ Software)

Backup dan Recovery Data

Sistem *backup* data dilakukan setiap hari secara otomatis pada pukul 02.00-04.00 WIB. Terdapat dua lapisan backup yaitu *backup live* di *server cloud* vendor (yang memungkinkan pemulihan data *real-time*) dan backup harian di server internal rumah sakit (data H-1). *Server cloud* vendor menjamin ketersediaan 99,99% dengan server cadangan yang siap aktif otomatis. Target RTO ditetapkan 30 menit untuk server cloud dan maksimal 60 menit untuk pemulihan penuh.

Kelemahan yang ditemukan adalah bahwa proses uji coba *restore* (*restore test*) belum pernah dilakukan secara formal untuk memverifikasi keberhasilan dan kelengkapan data backup. P03.2 mengakui hal ini:

"Kita jujur belum pernah melakukan tes recovery langsung untuk terhadap data backup kita kita hanya sebatas melakukan backup biar berhasil sudah selesai apa semua. Belum pernah, karena memang ada masalah untuk di infra hidup untuk masalah itu."-P03.2, Petugas IT (PJ Software)

Saat terjadi *downtime*, petugas menggunakan prosedur manual kemudian menginput ulang ke sistem setelah sistem pulih, sebagaimana dikonfirmasi P03.1:

"Dampaknya adalah layanan tetap berlanjut ketika terjadi downtime itu ke manual ketika sistem sudah menyala kembali file catatan secara manual itu di upload ke aplikasi RME."-P03.1, Petugas IT (PJ Keamanan)

Analisis Potensi Ancaman dan Risiko Cyber Security terhadap RME

Malware

RSJ Dr. Soeharto Heerdjan pernah mengalami insiden infeksi *malware* pada komputer *workstation*. *Endpoint protection* (*next-generation antivirus*) yang terpasang berhasil mendeteksi dan memblokir file *malware* secara otomatis sebelum menginfeksi sistem RME. Sistem *log antivirus* mencatat laporan serangan yang diterima secara rutin oleh tim IT. P01 (Kepala RM) juga pernah mengalami insiden virus yang menyebabkan sistem berjalan lambat selama sekitar satu bulan. Berikut kutipan menjelaskan frekuensi ancaman malware: "Infeksi malware untuk dia user ada, untuk kejadian sih sering untungya kita pakai antivirus ya, jadi

langsung ke hapus filenya tapi kalau kayak itu ada file lognya ada siapa aja, mungkin untuk serangan itu kita udah hampir setiap hari ya."-P03.1, Petugas IT (PJ Keamanan)

Mitigasi yang diterapkan meliputi larangan penggunaan *flashdisk* di komputer rumah sakit, larangan mengunduh aplikasi tidak resmi dan pembatasan penggunaan komputer hanya untuk keperluan kerja.

"Yang berhak menggunakan flashdisk hanya saya dan nurul (petugas RM bagian pelaporan) untuk menggunakan laporan. Kita pun sekarang udah gak menggunakan itu, kita paling sekarang sudah mengirim lewat email untuk menghindari pemasukan flashdisk di PC."-P01, Kepala Rekam Medis

Phishing

Tidak ditemukan insiden *phishing* yang secara langsung menargetkan *kredensial login* sistem RME. Namun, terdapat insiden phishing di luar RME yang pernah menimpa pegawai rumah sakit. Insiden ini melibatkan *link phishing* mengatasnamakan aktivasi KTP elektronik yang berujung pada kerugian finansial senilai sekitar Rp 500.000. Berikut kutipan yang menceritakan insiden tersebut:

"Iya sempet kehilangan sekitar 500 ribu, sudah lapor ke kepolisian juga, berupa uang bukan data ya, karena setiap yang kalau setelah instal itu dia dapat email itu dari BNI untuk perubahan datanya."-P03.1, Petugas IT (PJ Keamanan)

Edukasi dan pencegahan phishing dilakukan melalui security awareness training sebanyak dua kali setahun dalam format webinar (zoom). Namun, belum pernah dilakukan simulasi phishing (phishing simulation test) untuk mengukur tingkat kewaspadaan pegawai.

"kita setiap setahun dua kali melakukan security awareness informasi... Edukasinya melalui zoom atau pelatihan sebenarnya kita dapet saran kalau besar kita mau melakukan uji coba kita pake nomor orang lain terus kita ngirim atas nama rumah sakit kita bikin web jebakan sih apakah mereka masukin juga... tapi untuk saat ini direksi belum mau."-P03.1, Petugas IT (PJ Keamanan)

Serangan DoS/DdoS

Hingga saat ini, RSJ Dr. Soeharto Heerdjan belum pernah mengalami serangan DoS/DDoS yang menyebabkan *downtime* sistem RME dalam jangka panjang. Tim IT pernah melakukan uji coba penetrasi pada fitur login untuk mengevaluasi ketahanan terhadap serangan *brute force*. Hasil pengujian tersebut mendorong rekomendasi penambahan *captcha* dan waktu jeda (*rate limiting*) pada *form login*. P03.1 menjelaskan pengalaman pengujian tersebut: "Untuk saat ini belum tapi untuk kita melakukan testing pernah. Kita kalau DOS itu bagian login, dikarenakan disetting untuk menginjeksi password username berkali-kali. Itu makanya

waktu pas penemuan minta ketika mereka tiga kali atau lima kali isi password ada waktu jeda untuk mengatasi atau menggunakan captcha."

Mitigasi yang ada saat ini mengandalkan *firewall* yang secara otomatis memblokir koneksi yang melakukan *brute force*, serta pembagian VLAN untuk membatasi lalu lintas jaringan. SOP *downtime* telah disiapkan untuk kondisi sistem tidak dapat diakses lebih dari 20 menit.

Insider Threats

Ancaman dari dalam (*insider threats*) merupakan risiko terbesar yang diidentifikasi di RSJ Dr. Soeharto Heerdjan. Kasus yang ditemukan antara lain yaitu peminjaman akun login antar pengguna, terutama oleh dokter yang tidak dapat hadir namun membutuhkan input data, penyimpanan password di *browser* komputer bersama (fitur *autosave password*) dan tidak melakukan *logout* setelah selesai menggunakan sistem. P03.1 mengakui keberadaan masalah peminjaman akun ini:

"Pernah itu biasanya ternyata entah perawat atau dokter suka meminjamkan akun juga orang lain... Untuk saat ini kita lagi nerapin untuk penginputan tindakan atau CPPT itu hanya bisa menggunakan fingerprint atau face recognition."

P03.2 menyatakan bahwa ancaman internal merupakan risiko terbesar saat ini:

"Saya pribadi sih internal aja ya... kita berusaha nutupin celah yang ada di luar dan itu udah benar tapi ternyata yang ngerusak itu sebenarnya daripada orang dalamnya aja sih sebenarnya kayak gitu. Iya, gede karena mereka bisa melihat semua data-data pasien."

Respons terhadap ancaman ini adalah dengan menerapkan autentikasi biometrik (fingerprint) untuk input CPPT yang sedang dalam tahap implementasi, serta security awareness berkala setiap 3 bulan oleh P03.2.

Man-in-the-Middle (MitM) Attack

Risiko serangan MitM diminimalisir melalui pembatasan akses RME yang hanya dapat dilakukan dari dalam jaringan rumah sakit. Transmisi data menggunakan protokol HTTPS. Sistem hanya dapat diakses dari IP publik rumah sakit yang telah terdaftar. Akses dari luar harus menggunakan VPN dengan permohonan resmi dan jangka waktu terbatas. P04.2 mengonfirmasi bahwa sistem tidak dapat diakses dari luar rumah sakit:

"Nggak bisa. Kalau buka link ini harus di rumah sakit. Kita keluar pager aja nggak bisa. Ya, di depannya udah nggak bisa. Begitu pun untuk absen. Kita satu meter di luar rumah sakit nggak bisa akses untuk RME." Hingga saat ini belum pernah terdeteksi upaya penyadapan data pasien melalui jaringan. Enkripsi *end-to-end* belum sepenuhnya diterapkan pada seluruh

komunikasi sistem, sebagaimana disampaikan P03.2: "Kayaknya belum sampai kesana deh coba lanjut aja, belum."

Pembahasan

Penerapan Aspek Keamanan dan Kerahasiaan RME

Berdasarkan hasil penelitian, RSJ Dr. Soeharto Heerdjan telah menerapkan tujuh aspek keamanan informasi, yaitu *confidentiality*, *integrity*, *availability*, *authentication*, *access control*, *authorization*, dan *non-repudiation*. Pada aspek *confidentiality*, sistem menggunakan *username* dan *password* individual serta enkripsi SHA-256 pada sebagian data, tetapi masih ditemukan penggunaan *password* sederhana oleh sekitar 20% pengguna dan penyimpanan *password* pada *browser* komputer bersama. Temuan ini menunjukkan bahwa kerahasiaan data masih dipengaruhi oleh kedisiplinan pengguna dan belum sepenuhnya optimal. Pada aspek *integrity*, data dikunci setelah 1×24 jam dan setiap perubahan tercatat dalam *log*, tetapi validasi data masih dilakukan secara manual dan belum terdapat SOP khusus pengisian RME sehingga risiko *human error* masih ditemukan. Aspek *availability* tergolong baik karena didukung *server cloud* dengan *uptime* 99,99%, *backup* otomatis harian, server cadangan, serta target *Recovery Time Objective* (RTO) 30–60 menit. Pada aspek *authentication*, digunakan *username* dan *password* dengan pergantian setiap 90 hari serta sedang dikembangkan autentikasi biometrik, tetapi *Multi-Factor Authentication* (MFA) belum diterapkan secara menyeluruh. Aspek *access control* telah diterapkan melalui *Role-Based Access Control* (RBAC) dan pembatasan akses berdasarkan IP, sedangkan *authorization* dilakukan dengan membatasi hak edit dan penghapusan data sesuai kewenangan. Pada aspek *non-repudiation*, sistem telah memiliki *audit trail* yang mencatat pengguna, waktu, dan aktivitas, tetapi pemantauannya masih bersifat reaktif dan hanya dapat diakses oleh *super admin*. Secara keseluruhan, penerapan keamanan dan kerahasiaan RME telah berjalan cukup baik, tetapi masih memerlukan penguatan autentikasi, validasi data, pengawasan *audit trail*, dan kedisiplinan pengguna.

Evaluasi Penerapan Prinsip-Prinsip Cyber Security

Hasil penelitian menunjukkan bahwa penerapan prinsip *cyber security* di RSJ Dr. Soeharto Heerdjan meliputi *firewall*/*Intrusion Detection System* (IDS), enkripsi data, serta *backup* dan *recovery*. Pada aspek *firewall* dan IDS, rumah sakit menerapkan pertahanan berlapis melalui segmentasi VLAN, *firewall* rumah sakit dan vendor *cloud*, pembatasan IP yang di-*whitelist*, serta *endpoint protection* pada *workstation*. Namun, pemantauan *log* keamanan belum dilakukan secara rutin dan masih bersifat reaktif. Pada aspek enkripsi, digunakan SHA-256 untuk sebagian data dalam *database* dan HTTPS untuk transmisi data,

tetapi enkripsi belum mencakup seluruh data sensitif dan belum dilakukan evaluasi formal oleh pihak internal karena pengelolaannya berada pada vendor. Sementara itu, sistem *backup* dan *recovery* telah berjalan melalui *backup live* pada *server cloud* dan *backup* harian pada server internal dengan target RTO 30–60 menit. Temuan penting menunjukkan bahwa *restore test* belum pernah dilakukan secara formal, sehingga keberhasilan proses pemulihan data belum dapat dipastikan. Dengan demikian, prinsip *cyber security* telah diterapkan melalui infrastruktur keamanan berlapis, tetapi masih diperlukan pemantauan rutin, evaluasi enkripsi, serta pengujian *recovery* secara berkala.

Analisis Potensi Ancaman dan Risiko Cyber Security

Berdasarkan hasil penelitian, ancaman dan risiko *cyber security* pada RME RSJ Dr. Soeharto Heerdjan terdiri atas ancaman eksternal dan internal. Ancaman eksternal meliputi *malware*, *phishing*, dan DoS/DDoS, sedangkan ancaman internal meliputi *insider threats* dan risiko *Man-in-the-Middle* (MitM).

Ancaman dari Luar (External Threats): Malware, Phishing, dan DoS/DDoS

Hasil penelitian menunjukkan bahwa *malware* merupakan ancaman yang hampir setiap hari ditemukan pada *workstation*. Namun, *endpoint protection* mampu mendeteksi dan memblokir *malware* sebelum menginfeksi sistem RME. Rumah sakit juga menerapkan larangan penggunaan *flashdisk* dan pengunduhan aplikasi tidak resmi sebagai langkah pencegahan. Ancaman *phishing* belum pernah secara langsung menyerang kredensial RME, tetapi pernah dialami pegawai dan menimbulkan kerugian finansial. Rumah sakit telah melaksanakan *security awareness training* dua kali setahun, meskipun belum disertai simulasi *phishing*. Sementara itu, serangan DoS/DDoS belum pernah menyebabkan *downtime* berkepanjangan, tetapi hasil uji penetrasi internal menemukan kerentanan *brute force* pada fitur *login*. Temuan tersebut menunjukkan perlunya penerapan *captcha* dan *rate limiting* untuk memperkuat keamanan proses *login*.

Ancaman dari Dalam (Insider Threats) dan Risiko Man-in-the-Middle (MitM)

Hasil penelitian menunjukkan bahwa *insider threats* merupakan risiko yang paling nyata di RSJ Dr. Soeharto Heerdjan. Temuan yang ditemukan meliputi peminjaman akun *login*, penyimpanan *password* melalui fitur *auto-save browser* pada komputer bersama, dan kebiasaan tidak melakukan *logout*. Kondisi tersebut menunjukkan bahwa faktor manusia masih menjadi titik lemah dalam keamanan RME. Implementasi autentikasi biometrik *fingerprint* untuk input CPPT menjadi salah satu upaya mengurangi risiko peminjaman akun, tetapi perlu didukung kebijakan keamanan dan penegakan disiplin yang lebih kuat. Sementara itu, risiko MitM relatif telah diminimalkan melalui pembatasan akses RME dari jaringan internal rumah

sakit, penggunaan HTTPS, serta VPN untuk akses dari luar. Hingga penelitian dilakukan, belum ditemukan penyadapan data pasien melalui jaringan. Namun, belum diterapkannya enkripsi *end-to-end* secara menyeluruh masih menjadi celah yang perlu diperhatikan karena data pasien, khususnya data pasien gangguan jiwa, memiliki tingkat sensitivitas yang tinggi.

5. KESIMPULAN DAN SARAN

Dari hasil penelitian yang telah dilakukan di RSJ Dr. Soeharto Heerdjan, peneliti menarik kesimpulan sebagai berikut: Penerapan Aspek Keamanan dan Kerahasiaan RME: RSJ Dr. Soeharto Heerdjan telah menerapkan ketujuh aspek keamanan dan kerahasiaan RME (*confidentiality, integrity, availability, authentication, access control, authorization, dan non-repudiation*), namun belum seluruhnya berjalan optimal. Aspek *integrity* dan *availability* menunjukkan penerapan yang relatif baik melalui mekanisme penguncian data 1x24 jam dan dukungan *server cloud* bergaransi tinggi, sedangkan aspek *confidentiality, authentication, authorization, dan non-repudiation* masih memerlukan peningkatan signifikan, terutama terkait penguatan kebijakan *password*, implementasi MFA, formalisasi *workflow* otorisasi, dan optimalisasi pemanfaatan *audit trail* secara *proaktif*.

Evaluasi Penerapan Prinsip-Prinsip *Cyber Security*: Prinsip-prinsip *cyber security* yang meliputi *firewall/IDS*, enkripsi data, dan *backup-recovery* sudah diterapkan di RSJ Dr. Soeharto Heerdjan dengan tingkat kelengkapan yang bervariasi. *Firewall* berlapis dan segmentasi VLAN sudah berjalan baik, tetapi *log monitoring* keamanan belum dilakukan secara rutin harian. Enkripsi data baru mencakup sebagian field dan belum pernah dievaluasi secara formal. *Backup* harian otomatis sudah berjalan, tetapi uji coba *restore (restore test)* belum pernah dilaksanakan sehingga keandalan proses pemulihan data belum dapat diverifikasi sepenuhnya. Analisis Potensi Ancaman dan Risiko *Cyber Security*: Dari lima jenis ancaman yang dianalisis, *insider threats* merupakan risiko terbesar dan paling nyata, ditandai dengan peminjaman akun antar pengguna, penyimpanan *password* di *browser* komputer bersama, dan kebiasaan tidak *logout*. Ancaman *malware* terjadi hampir setiap hari namun berhasil diblokir oleh *endpoint protection*. *Phishing* pernah terjadi di luar sistem RME dan belum ada simulasi *phishing* untuk mengukur kewaspadaan pegawai. Serangan DoS/DDoS dan MitM belum pernah terjadi, namun kerentanan pada *form login* dan enkripsi yang belum menyeluruh tetap menjadi potensi risiko yang perlu diantisipasi. Secara keseluruhan, aspek kesadaran dan kepatuhan SDM terhadap kebijakan keamanan data menjadi tantangan utama yang dihadapi oleh rumah sakit.

DAFTAR REFERENSI

- Ahmad, A., Hastuti, J., Hijriatin, M., & Sarno, S. (2025). Data security analysis in electronic health information systems. *Journal Informatic, Education and Management (JIEM)*, 7(1), 1–11. <https://doi.org/10.61992/jiem.v7i1.107>
- Ariani Suci. (2023). Analisis keberhasilan implementasi rekam medis elektronik dalam meningkatkan efisiensi dan mutu pelayanan. *Analisis Keberhasilan Implementasi Rekam Medis Elektronik dalam Meningkatkan Efisiensi dan Mutu Pelayanan*, 2(2), 7–14.
- Herdadi, A. (2024). Analisis keamanan siber pada implementasi sistem informasi rekam medis OpenEMR V7.0.2. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, 7(4), 824–833. <https://doi.org/10.32672/jnkti.v7i4.7887>
- Hutauruk, P. M., & Astuti, W. T. (2018). Tinjauan aspek keamanan dan kerahasiaan dokumen rekam medis di ruang filling Rumah Sakit Khusus (RSK) Paru Medan tahun 2018. *Jurnal Ilmiah Perkam dan Informasi Kesehatan Imelda*, 3(2), 510–518.
- Kementerian Kesehatan Republik Indonesia. (2022). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis*.
- Mahendra, A. R., Siswati, Sonia, D., & Iqbal, M. F. (2025). Tinjauan sistem keamanan rekam medis elektronik di Rumah Sakit Al Dr. Mintohardjo Jakarta. *VitaMedica: Jurnal Rumpun Kesehatan Umum*, 3, 75–90.
- Min-Fang, T., Shin-Yuan, H., Wen-Ju, Y., C. C., C., & C., Y. D. (2019). Understanding physicians' adoption of electronic medical records: Healthcare technology self-efficacy, service level and risk perspectives. *Computer Standards & Interfaces*, 66, 1–11. <https://doi.org/10.1016/j.csi.2019.04.001>
- Nugroho, M. R. P., & Kurniadi, A. (2022). Tinjauan tata kelola keamanan RME berdasarkan prinsip keamanan PMK No. 24 Tahun 2022 di RSUD Dr. H. Soewondo Kendal. *Manajemen Informasi Kesehatan Indonesia*, 13(1), 25–33.
- Ramadhani, T. A., Cobantroro, A. F., & Sugianti. (2024). Implementasi algoritma Advanced Encryption Standard 128 untuk pengamanan database sistem. *Jurnal Informatika Polinema*, 10, 521–526.
- Rani, D. M., Widyaningrum, B. N., & Rizqulloh, L. (2024). Edukasi mengenai aspek keamanan informasi data pasien pada penerapan RME di RSI Sultan Agung. *PAKDEMAs: Jurnal Pengabdian Kepada Masyarakat*, 115–120. <https://jurnal.faperta-unras.ac.id/index.php/pakdemas/article/view/328>
- Republik Indonesia. (2023). *Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 tentang Kesehatan*.
- Setyaningrum, E., & Ricky, A. V. (2025). Analisis keamanan data pasien dalam rekam medis elektronik berdasarkan CIA Triad di RSUD X Jawa Tengah. *Jurnal Ners*, 9(3), 4216–4221. <https://doi.org/10.31004/jn.v9i3.46352>
- Suhariyono, U. S., Ikawati, F. R., & 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.
- Tiorentap, D. R. A., & Hosizah, H. (2020). Aspek keamanan informasi dalam penerapan rekam medis elektronik di Klinik Medical Check-Up MP. *SENWODIPA*, 53–66.

- Wardani, E., Putra, D. H., Sonia, D., Yulia, N., & Abstrak, K. K. (2024). Keamanan sistem informasi rekam medis elektronik di Rumah Sakit Islam Jakarta Sukapura. *Jurnal Rekam Medik dan Manajemen Informasi Kesehatan*, 3(2), 2829–4777.
- We'e, A., Nugroho, R. H., & Siswatibudi, H. (2023). Evaluasi aspek keamanan dan kerahasiaan rekam medis elektronik di Rumah Sakit Panti Nugroho. *Jurnal Permata Indonesia*, 14(2), 72–81. <https://doi.org/10.59737/jpi.v14i2.265>
- Wirajaya, M. K. M., & Dewi, N. M. U. K. (2020). Analisis kesiapan Rumah Sakit Dharma Kerti Tabanan menerapkan rekam medis elektronik. *Jurnal Kesehatan Vokasional*, 5(1), 1. <https://doi.org/10.22146/jkesvo.53017>