Jurnal Ilmiah Sistem Informasi dan Ilmu Komputer
Volume. 6 Nomor. 2 Juli 2026
e-ISSN: 2827-8135; e-ISSN: 2827-7953; Hal 645-655
DOI: https://doi.org/10.55606/juisik.v6i2.2587
Tersedia: https://journal.sinov.id/index.php/juisik

Evaluasi Keamanan Rekam Medis Elektronik pada Rumah Sakit X

Sayidatun Nisa Rushdiya Nayyara[1*], Fita Rusdian Ikawati[2], Untung Slamet Suhariyono[3]
[1-3]Program Studi D-III Rekam Medis dan Informasi Kesehatan, Institut Teknologi Sains dan Kesehatan RS dr. Soepraoen Kesdam V/BRW Malang, Indonesia
**Penulis Korespondensi: rarasayidatun@gmail.com*

Abstract. *Electronic Medical Records (EMR) have become a mandatory component of digital health transformation in Indonesian hospitals, yet their implementation introduces information security risks that directly affect hospital quality management and patient trust. This study aimed to evaluate the security level of the EMR system at X Hospital based on the ISO/IEC 27001:2022 standard and the Indonesian Minister of Health Regulation No. 24 of 2022. A descriptive quantitative method with a Gap Analysis approach was employed, involving 54 respondents from three work units selected through total sampling, using a closed questionnaire adapted from 93 ISO/IEC 27001:2022 security controls, supported by direct observation and documentation review. The results show that overall EMR security reached a good category at 77.3 percent, with an average gap of 22 percent classified as small compared to the ideal standard. The largest gaps were identified in People Controls and the Availability aspect, indicating that human resource management and system continuity planning remain the weakest areas. These findings imply that hospital management should prioritize cybersecurity training, stricter password policies, and the development of disaster recovery and business continuity plans to strengthen EMR security and support compliance with national and international standards.*

Keywords: *Electronic Medical Record; Gap Analysis; Hospital; Information Security; ISO/IEC 27001:2022.*

Abstrak. Rekam Medis Elektronik (RME) telah menjadi komponen wajib dalam transformasi digital layanan kesehatan di rumah sakit Indonesia, namun penerapannya menimbulkan risiko keamanan informasi yang berdampak langsung pada manajemen mutu rumah sakit dan kepercayaan pasien. Penelitian ini bertujuan mengevaluasi tingkat keamanan sistem RME di Rumah Sakit X berdasarkan standar ISO/IEC 27001:2022 dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022. Penelitian menggunakan metode deskriptif kuantitatif dengan pendekatan Gap Analysis, melibatkan 54 responden dari tiga unit kerja yang dipilih melalui total sampling, menggunakan kuesioner tertutup yang diadaptasi dari 93 kontrol keamanan ISO/IEC 27001:2022, didukung observasi langsung dan studi dokumentasi. Hasil penelitian menunjukkan bahwa keamanan RME secara keseluruhan berada pada kategori baik dengan capaian 77,3 persen, dengan rata-rata gap sebesar 22 persen yang tergolong kecil terhadap standar ideal. Kesenjangan terbesar ditemukan pada aspek People Controls dan Availability, menunjukkan bahwa pengelolaan sumber daya manusia dan perencanaan keberlangsungan sistem masih menjadi area terlemah. Temuan ini mengimplikasikan bahwa manajemen rumah sakit perlu memprioritaskan pelatihan keamanan siber, kebijakan kata sandi yang lebih ketat, serta penyusunan rencana pemulihan bencana dan keberlangsungan bisnis guna memperkuat keamanan RME dan mendukung kepatuhan terhadap standar nasional maupun internasional.

Kata Kunci: Gap Analysis; Analysis ISO/IEC 27001:2022; Keamanan Informasi; Rekam Medis Elektronik; Rumah Sakit.

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi yang pesat telah mengubah pelayanan kesehatan di berbagai negara, termasuk Indonesia, dengan mendorong peralihan dari sistem pencatatan berbasis kertas menuju sistem elektronik. Pemanfaatan teknologi informasi telah menjadi kebutuhan penting dalam mendukung kinerja organisasi layanan kesehatan (Ikawati, 2024), dan terbukti memberikan manfaat berupa peningkatan kualitas layanan, penurunan kesalahan medis, kemudahan akses informasi, serta optimalisasi pemantauan ketersediaan fasilitas (Amin et al., 2021). Rekam Medis Elektronik (RME) merupakan salah

Naskah Masuk: 09 Mei 2026; Revisi: 10 Juni 2026; Diterima: 11 Juli 2026; Tersedia: 21 Juli 2026

satu wujud transformasi tersebut, berperan memodernisasi pengelolaan informasi medis, meningkatkan efisiensi manajemen, serta mendukung pelayanan pasien yang berkualitas (Tiorentap, 2020). Di Indonesia, penerapan RME diwajibkan melalui Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 sebagai bagian dari transformasi digital sektor kesehatan (Kementerian Kesehatan RI, 2022). Namun demikian, implementasi RME menimbulkan tantangan keamanan informasi yang erat kaitannya dengan manajemen mutu rumah sakit, sehingga dibutuhkan tata kelola yang baik untuk menjamin keamanan data (Sofia et al., 2022). Sistem keamanan yang lemah, seperti kurangnya pelatihan siber, evaluasi kebijakan, dan pengawasan, dapat mencerminkan rendahnya mutu manajemen serta berpotensi mengakibatkan kebocoran data rekam medis pasien yang menimbulkan kerugian finansial, hilangnya kepercayaan publik, dan potensi sanksi hukum (Rusdi & Ularan, 2023).

Beberapa penelitian terdahulu telah mengkaji penerapan keamanan informasi pada sistem RME di berbagai fasilitas pelayanan kesehatan. Penelitian pada suatu fasilitas kesehatan menunjukkan bahwa dari aspek kerahasiaan, sistem telah menggunakan login dengan username dan password, namun belum dilakukan penggantian berkala dan belum tersedia Standard Operating Procedures (SOP) yang mengatur mekanisme tersebut, sementara dari aspek integritas masih terdapat fitur pengeditan data yang dapat diakses pengguna (Ardianto et al., 2024). Penelitian lain pada Klinik Medical Check-Up MP mengungkapkan bahwa pencapaian aspek keamanan seperti kerahasiaan, integritas, autentikasi, ketersediaan, kontrol akses, dan non-repudiation masih berada di bawah standar karena belum dilakukan audit internal maupun eksternal sesuai kerangka ISO/IEC 27001:2022 (Tiorentap & Hosizah, 2020). Studi lain juga menegaskan bahwa sektor kesehatan merupakan salah satu sektor paling rentan terhadap serangan siber karena informasi pasien yang sangat lengkap dan sensitif, sehingga sistem keamanan data di rumah sakit dinilai masih belum memadai dan berisiko terhadap pelanggaran privasi pasien (Rani & Widyaningrum, 2025). Pelanggaran keamanan tersebut dapat berdampak serius, baik secara finansial akibat denda regulasi dan biaya pemulihan (Rusdi & Ularan, 2023), maupun secara operasional berupa kelumpuhan sistem informasi rumah sakit yang mengganggu alur pelayanan dan menurunkan kualitas pelayanan kepada pasien (Tiorentap & Hosizah, 2020), termasuk ancaman serangan ransomware yang dapat membahayakan keselamatan pasien (Wardani, 2024).

Dari uraian tersebut terlihat bahwa penelitian-penelitian terdahulu umumnya masih bersifat parsial, baik hanya menyoroti sebagian aspek keamanan informasi saja, terbatas pada satu unit kerja, maupun belum mengaitkan hasil evaluasi secara eksplisit dengan dua acuan sekaligus, yaitu standar internasional ISO/IEC 27001:2022 dan regulasi nasional Permenkes

Nomor 24 Tahun 2022. Kesenjangan (gap) inilah yang mendasari urgensi penelitian ini, yaitu perlunya evaluasi keamanan RME yang bersifat komprehensif, melibatkan seluruh pengguna dari berbagai unit kerja, serta menggunakan pendekatan yang dapat mengukur besaran kesenjangan secara kuantitatif antara kondisi aktual dan kondisi ideal berdasarkan kedua acuan tersebut. Kebaruan penelitian ini terletak pada penggunaan metode deskriptif kuantitatif dengan pendekatan Gap Analysis yang mengadaptasi 93 kontrol keamanan dari ISO/IEC 27001:2022 dan melibatkan seluruh pengguna RME dari tiga unit kerja di lokasi penelitian.

Berdasarkan latar belakang dan kesenjangan tersebut, penelitian ini bertujuan untuk mengevaluasi keamanan sistem RME di Rumah Sakit X berdasarkan standar ISO/IEC 27001:2022 dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022, guna mengidentifikasi aspek yang memiliki kesenjangan terbesar dan merumuskan rekomendasi perbaikan yang spesifik dan aplikatif untuk peningkatan keamanan data pasien.

2. KAJIAN TEORITIS

Rekam Medis Elektronik (RME) merupakan sistem digital yang digunakan untuk mencatat, menyimpan, dan mengelola informasi medis pasien secara terstruktur, menggantikan sistem pencatatan manual berbasis kertas. Penerapan RME memberikan manfaat berupa peningkatan efisiensi pelayanan, penurunan kesalahan medis, serta kemudahan akses informasi pasien secara real-time (Tiorentap, 2020). RME juga berperan penting dalam mendukung kualitas pengambilan keputusan klinis karena data pasien tersimpan secara terintegrasi dan dapat diakses oleh tenaga kesehatan yang berwenang (Amin et al., 2021). Di Indonesia, penerapan RME diatur secara resmi melalui Peraturan Menteri Kesehatan Nomor 24 Tahun 2022, yang mewajibkan seluruh fasilitas pelayanan kesehatan untuk beralih ke sistem rekam medis elektronik sebagai bagian dari transformasi digital sektor kesehatan (Kementerian Kesehatan RI, 2022).

Keamanan informasi merupakan upaya melindungi kerahasiaan, keutuhan, dan ketersediaan data dari ancaman baik internal maupun eksternal. Dalam konteks RME, keamanan informasi menjadi krusial karena data yang dikelola bersifat sangat sensitif dan menyangkut privasi pasien (Sofia et al., 2022). Tiga prinsip utama keamanan informasi — Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan), dikenal sebagai CIA Triad, menjadi landasan pengaturan keamanan RME dalam Permenkes Nomor 24 Tahun 2022 Pasal 29 (Kementerian Kesehatan RI, 2022). Confidentiality memastikan data hanya diakses pihak berwenang, Integrity menjamin data tetap akurat dan tidak berubah tanpa

izin, sedangkan Availability memastikan data dapat diakses saat dibutuhkan oleh pengguna yang sah (Ardianto et al., 2024).

ISO/IEC 27001:2022 merupakan standar internasional untuk Sistem Manajemen Keamanan Informasi (SMKI) yang memberikan kerangka kerja sistematis dalam mengelola risiko keamanan informasi suatu organisasi (International Organization for Standardization, 2022). Standar ini mencakup 93 kontrol keamanan yang dikelompokkan ke dalam empat kategori utama: Organisational Controls, People Controls, Physical Controls, dan Technological Controls. Penerapan ISO/IEC 27001:2022 pada institusi kesehatan bertujuan memastikan pengelolaan data pasien, termasuk RME, memenuhi standar keamanan informasi yang diakui secara global sekaligus selaras dengan regulasi nasional (Prasetyo & Widodo, 2023).

Gap Analysis merupakan metode evaluasi yang digunakan untuk mengidentifikasi dan mengukur kesenjangan antara kondisi aktual suatu sistem dengan kondisi ideal yang ditetapkan oleh suatu standar atau regulasi (Djatmiko & Pradana, 2021). Dalam konteks keamanan informasi, Gap Analysis digunakan untuk menilai sejauh mana implementasi kontrol keamanan yang berjalan telah memenuhi persyaratan standar acuan, sehingga dapat diketahui area yang memerlukan perbaikan prioritas (Wahyuni & Santoso, 2021). Hasil Gap Analysis umumnya dikategorikan ke dalam tiga tingkatan: gap kecil (<50%) yang menunjukkan implementasi sudah mendekati kondisi ideal, gap sedang (50–75%) yang masih memerlukan perbaikan berkelanjutan, dan gap besar (>75%) yang menunjukkan standar belum diterapkan dengan baik (Wahyuni & Santoso, 2021).

Beberapa penelitian terdahulu telah mengkaji penerapan keamanan informasi pada sistem RME di berbagai fasilitas pelayanan kesehatan dan menjadi landasan bagi penelitian ini. Ardianto et al. (2024) menemukan bahwa dari aspek kerahasiaan, sistem RME telah menggunakan login dengan username dan password, namun belum dilakukan penggantian berkala dan belum tersedia SOP yang mengatur mekanisme tersebut, sementara dari aspek integritas masih terdapat fitur pengeditan data yang dapat diakses pengguna. Tiorentap dan Hosizah (2020) dalam penelitiannya pada Klinik Medical Check-Up MP mengungkapkan bahwa pencapaian aspek keamanan seperti kerahasiaan, integritas, autentikasi, ketersediaan, kontrol akses, dan non-repudiation masih berada di bawah standar karena belum dilakukan audit internal maupun eksternal sesuai kerangka ISO/IEC 27001. Sementara itu, Rani dan Widyaningrum (2025) menegaskan bahwa sektor kesehatan merupakan salah satu sektor paling rentan terhadap serangan siber karena informasi pasien yang sangat lengkap dan sensitif, sehingga sistem keamanan data di rumah sakit dinilai masih belum memadai. Rusdi dan Ularan

(2023) menambahkan bahwa pelanggaran keamanan informasi kesehatan dapat menimbulkan kerugian finansial signifikan akibat denda regulasi, biaya pemulihan, serta hilangnya kepercayaan publik. Berdasarkan ulasan tersebut, penelitian-penelitian sebelumnya cenderung mengevaluasi aspek keamanan secara parsial dan pada satu unit kerja, sehingga penelitian ini diarahkan untuk melakukan evaluasi yang lebih komprehensif dengan mengacu pada dua standar sekaligus, yaitu ISO/IEC 27001:2022 dan Permenkes Nomor 24 Tahun 2022.

Berdasarkan kajian teori dan penelitian terdahulu tersebut, penelitian ini diarahkan pada dugaan bahwa implementasi keamanan sistem RME di Rumah Sakit X masih memiliki kesenjangan terhadap standar ISO/IEC 27001:2022 dan Permenkes Nomor 24 Tahun 2022, dengan kesenjangan yang diperkirakan lebih besar terjadi pada aspek People Controls dan Organisational Controls dibandingkan aspek Technological Controls, mengingat pola temuan serupa pada penelitian-penelitian sejenis sebelumnya.

3. METODE PENELITIAN

Penelitian ini menggunakan desain deskriptif kuantitatif dengan pendekatan Gap Analysis, yang dipilih karena mampu mengidentifikasi dan mengukur kesenjangan antara kondisi aktual dengan kondisi ideal secara objektif serta menghasilkan rekomendasi perbaikan yang terukur (Djatmiko & Pradana, 2021; Prasetyo & Widodo, 2023). Penelitian dilaksanakan di Rumah Sakit X, Kota Batu, Jawa Timur, pada periode Maret hingga Juni 2025, dengan populasi seluruh petugas pengguna Rekam Medis Elektronik (RME) di tiga unit kerja, yaitu Instalasi Gawat Darurat, Instalasi Rawat Jalan, dan Instalasi Medical Record, berjumlah 54 orang yang seluruhnya dijadikan responden melalui teknik Total Sampling karena populasi relatif kecil. Variabel penelitian adalah tingkat implementasi keamanan informasi RME pada aspek Confidentiality, Integrity, dan Availability sesuai Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 Pasal 29, yang diukur menggunakan skala skor 0 (belum diterapkan) hingga 3 (diterapkan sepenuhnya) (Ardianto et al., 2024). Instrumen penelitian berupa kuesioner tertutup yang diadaptasi dari 93 kontrol keamanan pada ISO/IEC 27001:2022 Annex A, sehingga validitas isi instrumen mengacu langsung pada standar internasional tersebut dan tidak memerlukan pengujian validitas empiris tambahan (International Organization for Standardization, 2022); pengumpulan data dilengkapi dengan observasi langsung terhadap sistem RME serta studi dokumentasi kebijakan dan SOP keamanan informasi sebagai data pendukung.

Analisis data dilakukan secara deskriptif kuantitatif dengan menentukan skor capaian setiap klausul, menjumlahkan skor per aspek, lalu menghitung persentase pemenuhan melalui

perbandingan antara skor yang diperoleh dari kuesioner responden dengan skor maksimal ideal apabila seluruh kontrol diterapkan sepenuhnya (54 responden × 93 item × skor 3), sebelum dibandingkan antar aspek dan disajikan dalam bentuk tabel dan diagram (Prasetyo & Widodo, 2023). Selanjutnya dilakukan Gap Analysis dengan menghitung persentase gap sebagai selisih antara seratus persen dan persentase pemenuhan yang telah diperoleh, kemudian dikategorikan menjadi gap kecil (di bawah 50%) yang menunjukkan implementasi sudah mendekati standar, gap sedang (50–75%) yang masih memerlukan peningkatan, dan gap besar (di atas 75%) yang menunjukkan standar belum diterapkan dengan baik, sebagai dasar penentuan prioritas perbaikan pada setiap aspek keamanan (Wahyuni & Santoso, 2021).

4. HASIL DAN PEMBAHASAN

Pengumpulan data dilakukan di Rumah Sakit X, Kota Batu, Jawa Timur, pada periode Maret hingga Juni 2025, melalui kuesioner tertutup kepada 54 responden dari tiga unit kerja, dilengkapi observasi langsung terhadap sistem RME serta studi dokumentasi kebijakan dan SOP keamanan informasi.

Evaluasi Keamanan RME Berdasarkan Standar ISO/IEC 27001:2022

Evaluasi dilakukan terhadap empat aspek kontrol keamanan ISO/IEC 27001:2022, yaitu Organisational Controls, People Controls, Physical Controls, dan Technological Controls. Hasil rekapitulasi dari 54 responden dengan 93 item pertanyaan disajikan pada Tabel 1.

Tabel 1. Rekapitulasi Tingkat Keamanan RME Berdasarkan Standar ISO/IEC 27001:2022.

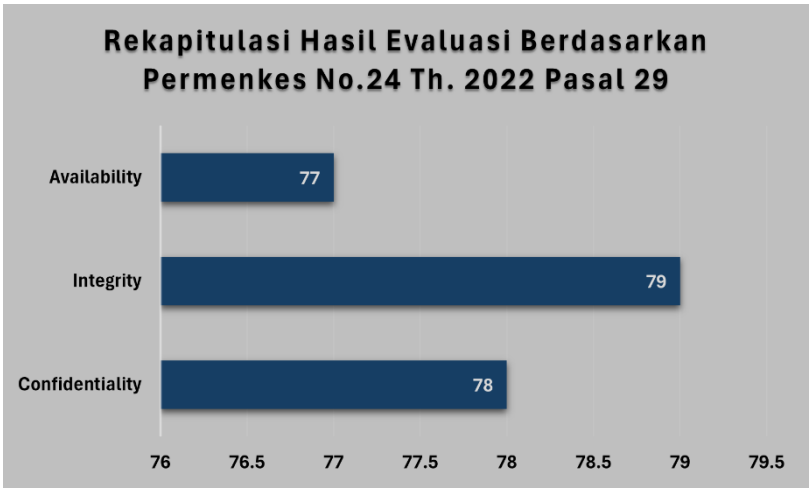
Aspek Kontrol	Skor Aktual	Skor Maksimal	Persentase (%)	Kategori
Organisational Controls	4.595	5.994	76,6	Baik
People Controls	957	1.296	73,8	Baik
Physical Controls	1.786	2.268	78,7	Baik
Technological Controls	4.418	5.508	80,2	Baik
Rata-rata	–	–	77,3	Baik

Sumber: Hasil Pengolahan Data Primer

Tabel 1 menunjukkan tingkat keamanan RME secara keseluruhan berada pada kategori Baik dengan rata-rata 77,3%. Physical Controls mencatat persentase tertinggi (78,7%), mengindikasikan kontrol keamanan fisik seperti pengamanan ruang server dan akses fisik ke area sensitif sudah diterapkan optimal, sementara People Controls mencatat persentase terendah (73,8%), menunjukkan pengelolaan sumber daya manusia terkait keamanan informasi khususnya pelatihan keamanan siber dan manajemen kompetensi petugas masih perlu ditingkatkan.

Evaluasi Keamanan RME Berdesarkan Aspek Permenkes No.24 Tahun 2022

Berdasarkan Pasal 29 Permenkes No. 24 Tahun 2022, evaluasi dilakukan pada tiga prinsip: Confidentiality, Integrity, dan Availability, sebagaimana disajikan pada Gambar 1.



Gambar 1. Perbandingan Persentase Pencapaian Aspek Confidentiality, Integrity, dan Availability.

Sumber: Hasil Pengolahan Data Primer

Aspek Integrity mencapai persentase tertinggi (79,4%) melalui mekanisme backup data rutin setiap awal bulan, meskipun sistem audit trail dan pencatatan log aktivitas belum berjalan optimal. Aspek Confidentiality mencapai 78,5%, didukung autentikasi username-password dan pembatasan akses berbasis unit kerja, namun belum menerapkan penggantian password berkala maupun autentikasi multi-faktor. Aspek Availability memperoleh capaian terendah (73,2%) — sistem berjalan stabil selama ada koneksi internet dan didukung UPS/genset, tetapi rumah sakit belum memiliki Disaster Recovery Plan maupun Business Continuity Plan yang komprehensif.

Keterkaitan Hasil dengan Dugaan Penelitian

Hasil ini konsisten dengan dugaan yang dikemukakan pada bagian Kajian Teoritis, yaitu kesenjangan diperkirakan lebih besar pada aspek People Controls dan Organisational Controls dibandingkan Technological Controls. Data pada Tabel 1 membuktikan hal tersebut: gap pada People Controls (26,2%) dan Organisational Controls (23,4%) memang lebih besar dibandingkan gap pada Technological Controls (19,8%), menegaskan bahwa kesenjangan keamanan RME lebih banyak bersumber dari faktor manusia dan tata kelola organisasi ketimbang keterbatasan teknologi.

Gap Analysis Keamanan RME terhadap Standar Permenkes No.24 Tahun 2022

Hasil Gap Analysis yang membandingkan kondisi aktual dengan kondisi ideal disajikan pada Tabel 2.

Tabel 2. Rekapitulasi Tingkat Keamanan RME Berdasarkan Standar ISO/IEC 27001:2022.

Aspek Kontrol	Kondisi Aktual (%)	Kondisi Ideal (%)	Gap (%)	Kategori
Confidentiality	78	100	22	Gap Kecil
Integrity	79	100	21	Gap Kecil
Availability	77	100	23	Gap Kecil
Rata-rata	78	100	22	Gap Kecil

Sumber: Hasil Pengolahan Data Primer

Tabel 2 menunjukkan rata-rata gap sebesar 22% antara kondisi aktual dengan standar ideal Permenkes No. 24 Tahun 2022, termasuk kategori Gap Kecil. Prioritas perbaikan perlu difokuskan pada aspek Availability (gap 23%), diikuti Confidentiality (22%) dan pemeliharaan berkelanjutan pada Integrity (21%).

Kesuaian dengan Penelitian Terdahulu

Hasil ini sejalan dengan Rani dan Widyaningrum (2025) di RSI Sultan Agung yang menunjukkan keamanan sistem berada pada kategori baik dengan capaian di atas 70%, namun bertentangan dengan Tiorentap dan Hosizah (2020) di Klinik Medical Check-Up MP yang mencatat capaian di bawah 60%. Perbedaan ini kemungkinan dipengaruhi oleh ketersediaan sumber daya, infrastruktur teknologi, dan tingkat kesadaran manajemen rumah sakit tipe C seperti Rumah Sakit X yang relatif lebih memadai dibandingkan fasilitas kesehatan primer.

Dampak Gap dan Implikasi

Secara teoritis, temuan ini memperkuat gambaran bahwa kesenjangan keamanan RME lebih dominan disebabkan faktor non-teknis (people dan organisational controls) dibandingkan faktor teknologi, sejalan dengan prinsip CIA Triad yang menekankan bahwa keamanan informasi bergantung pada manusia dan tata kelola, bukan semata infrastruktur. Secara terapan, gap pada Confidentiality (22%) berimplikasi pada risiko pelanggaran UU Perlindungan Data Pribadi sehingga memerlukan penguatan password policy dan autentikasi multi-faktor; gap pada Integrity (21%) berimplikasi pada risiko medico-legal akibat lemahnya audit trail, sehingga memerlukan SOP input data yang lebih ketat; sementara gap pada Availability (23%) — sebagai yang terbesar — berimplikasi pada risiko terhentinya layanan kritis seperti IGD apabila terjadi gangguan sistem, sehingga penyusunan Disaster Recovery Plan dan Business Continuity Plan menjadi rekomendasi prioritas bagi manajemen rumah sakit (Tiorentap & Hosizah, 2020).

5. KESIMPULAN DAN SARAN

Penelitian ini menjawab tujuan evaluasi keamanan sistem Rekam Medis Elektronik (RME) di Rumah Sakit X, dengan hasil menunjukkan bahwa implementasi keamanan telah berada pada kategori baik dan gap terhadap standar ISO/IEC 27001:2022 maupun Permenkes No. 24 Tahun 2022 tergolong kecil. Kesenjangan yang tersisa didominasi oleh faktor manusia dan tata kelola organisasi, bukan keterbatasan teknologi, sejalan dengan dugaan yang diajukan di awal penelitian. Temuan ini menegaskan bahwa kepatuhan terhadap standar keamanan informasi bukan semata soal kelengkapan infrastruktur, melainkan juga soal konsistensi kebijakan dan kesiapan sumber daya manusia dalam menjalankannya.

Berdasarkan temuan tersebut, Rumah Sakit X disarankan memprioritaskan penguatan pada aspek People Controls dan Availability, antara lain melalui pelatihan keamanan informasi yang terjadwal dan wajib, kebijakan penggantian password berkala disertai autentikasi multi-faktor, serta penyusunan dan pengujian Disaster Recovery Plan dan Business Continuity Plan untuk menjamin keberlangsungan layanan pada unit kritis seperti Instalasi Gawat Darurat.

Penelitian ini memiliki keterbatasan yang perlu diperhatikan dalam menginterpretasikan hasilnya. Evaluasi dilakukan pada satu rumah sakit tipe C dengan periode pengamatan yang relatif singkat, sehingga hasilnya tidak dapat digeneralisasikan secara langsung pada rumah sakit dengan tipe, skala, atau karakteristik sumber daya yang berbeda. Selain itu, data dikumpulkan melalui persepsi responden dan observasi pada satu titik waktu, sehingga belum menggambarkan dinamika keamanan informasi secara longitudinal maupun potensi bias persepsi dari petugas yang dievaluasi kinerjanya sendiri. Penelitian selanjutnya disarankan memperluas cakupan pada rumah sakit dengan tipe berbeda untuk menguji konsistensi pola temuan ini, serta mempertimbangkan pendekatan longitudinal atau audit independen guna memperkuat objektivitas hasil evaluasi keamanan informasi RME.

UCAPAN TERIMA KASIH

Penulis mengucapkan puji syukur kepada Allah SWT atas rahmat dan karunia-Nya sehingga penelitian ini dapat diselesaikan dengan baik. Penulis juga menyampaikan terima kasih kepada dosen pembimbing atas bimbingan dan arahan selama proses penelitian, kepada pihak Rumah Sakit X yang telah memberikan izin dan memfasilitasi pelaksanaan penelitian, kepada seluruh petugas rumah sakit yang telah berpartisipasi sebagai responden, serta kepada kedua orang tua atas doa, dukungan, dan motivasi yang senantiasa diberikan.

DAFTAR REFERENSI

Amin, M., Setyonugroho, W., & Hidayah, N. (2021). Implementasi rekam medik elektronik: Sebuah studi kualitatif. Jurnal Teknik Informatika dan Sistem Informasi (JATISI), 8(1), 430–442. http://jurnal.mdp.ac.id

Ardianto, E. T., Sabran, & Nurjanah, L. (2024). Analisis aspek keamanan data pasien dalam implementasi rekam medis elektronik di Rumah Sakit X. RAMMIK: Jurnal Rekam Medik dan Manajemen Informasi Kesehatan, 3(2), 18–30. https://doi.org/10.47134/rammik.v3i2.54

Djatmiko, T., & Pradana, R. (2021). Gap Analysis sebagai metode evaluasi kinerja organisasi. Jurnal Manajemen dan Bisnis, 8(1), 45–58.

Ikawati, F. R. (2024). Efektivitas penggunaan rekam medis elektronik terhadap peningkatan kualitas pelayanan pasien di rumah sakit. Ranah Research: Jurnal Riset Ranah, 6(3), 288–296. https://doi.org/10.38035/rrj.v6i3

International Organization for Standardization. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection: Information security management systems — Requirements. ISO.

Jayusman, I., & Shavab, O. A. K. (2020). Studi deskriptif kuantitatif tentang aktivitas belajar mahasiswa dengan menggunakan media pembelajaran Edmodo dalam pembelajaran sejarah. Jurnal Artefak, 7(1), 13–20. https://jurnal.unigal.ac.id/index.php/artefak

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis. Kementerian Kesehatan RI. https://peraturan.bpk.go.id/Details/245544/permenkes-no-24-tahun-2022

Prasetyo, D., & Widodo, A. (2023). Metode kuantitatif dalam analisis kesesuaian ISO/IEC 27001. Jurnal Sistem Informasi dan Manajemen, 9(1), 78–92.

Rani, D. M., & Widyaningrum, B. N. (2025). Evaluasi keamanan informasi sistem rekam medis elektronik di RSI Sultan Agung. Jurnal Manajemen Informasi Kesehatan, 10(1), 52–62.

Rusdi, A. J., & Ularan, R. A. R. (2023). Tinjauan literatur analisis yuridis manajemen kerahasiaan rekam medis elektronik. Jurnal Rekam Medis dan Informasi Kesehatan Indonesia (Jurmiki), 3(1), 64–69.

Sofia, S., Ardianto, E. T., Muna, N., & Sabran. (2022). Analisis aspek keamanan informasi pasien pada penerapan RME di fasilitas kesehatan. RAMMIK: Jurnal Rekam Medik dan Manajemen Informasi Kesehatan, 1(2), 94–103. https://doi.org/10.47134/rammik.v1i1.29

Tiorentap, D. R. A. (2020). Manfaat penerapan rekam medis elektronik di negara berkembang: Systematic literature review. Indonesian of Health Information Management Journal (INOHIM), 8(2), 69–79. https://doi.org/10.26555/inohim.v8i2

Tiorentap, D. R. A., & Hosizah. (2020). Aspek keamanan informasi dalam penerapan rekam medis elektronik di Klinik Medical Check-Up MP. Prosiding 4 SENWODIPA 2020, 53–60.

Wahyuni, S., & Santoso, B. (2021). Kategorisasi Gap Analysis dalam audit sistem manajemen keamanan informasi. Jurnal Teknologi Informasi dan Keamanan Sistem, 7(3), 234–248.

Wardani, E. (2024). Keamanan sistem informasi rekam medis elektronik di Rumah Sakit Islam Jakarta Sukapura. UEU Digital Repository. https://digilib.esaunggul.ac.id/UEU-Undergraduate-20210306012/38359/