SEHATRAKYAT (Jurnal Kesehatan Masyarakat)
https://journal.yp3a.org/index.php/sehatrakyat
DOI: 10.54259/sehatrakyat.v5i4.8622
e-ISSN 0852-1239 | p-ISSN 2829-9299
Vol. 5 No. 4 (November 2026) 1699-1707

Diterima Redaksi: 08-07-2026 | Selesai Revisi: 13-09-2026 | Diterbitkan Online: 15-11-2026

Analisis Keamanan Data Pasien pada Sistem Rekam Medis Elektronik di RSIJ Cempaka Putih

Agni Artika Nawawi[1], Bangga Agung Satrya[2], Noerfitri[3], Daniel Happy Putra[4]
[1,2,3,4]Program Studi Rekam Medis dan Informasi Kesehatan, Fakultas Ilmu-Ilmu Kesehatan, Universitas Esa Unggul, DKI Jakarta, Indonesia
Email: [1]agniartika09@gmail.com, [2]bangga.agung@esaunggul.ac.id, [3]noerfitri@esaunggul.ac.id, [4]daniel.putra@esaunggul.ac.id

Abstract

Adoption of Electronic Medical Records (EMR) brings clear gains in the efficiency of health service delivery, yet it simultaneously introduces new risks to the security of patient data. Safeguarding patient information is a core requirement for preserving its confidentiality, integrity, and availability. This research set out to examine how patient data security is implemented within the Electronic Medical Record system at RSIJ Cempaka Putih, using ISO/IEC 27001:2022 as the reference framework across organizational, human, physical, and technological dimensions, while also mapping the obstacles encountered and proposing improvements. A qualitative case-study design was applied. Five informants took part, namely the Head of Medical Records, two medical record staff, the Head of IT, and one IT staff member, all chosen through purposive sampling. Information was gathered via in-depth interviews, field observation, and document review, and subsequently examined using the Miles, Huberman, and Saldãna interactive analysis model. Findings indicate that RSIJ Cempaka Putih has put in place a range of information security measures, among them security policies, role-based user access control, downtime procedures, fingerprint-secured server room entry, and automated daily data backups. Even so, a number of gaps remain, including uneven security awareness among staff, occasional account sharing, a limited audit trail function, the lack of privacy screens at service points, and restricted CCTV coverage. Overall, patient data security at the hospital has been reasonably well implemented, though further strengthening is required in user awareness, policy adherence, and physical and technological controls to more fully meet ISO/IEC 27001:2022 requirements.

Keywords: *Patient Data Security, Electronic Medical Record, Hospital, Health Information System, ISO/IEC 27001:2022.*

Abstrak

Implementasi Rekam Medis Elektronik (RME) mendatangkan sejumlah manfaat bagi efisiensi layanan kesehatan, tetapi di sisi lain turut memunculkan risiko baru terhadap keamanan data pasien. Penelitian ini dilakukan untuk mengkaji bagaimana keamanan data pasien diterapkan pada Sistem RME di RSIJ Cempaka Putih dengan mengacu pada standar ISO/IEC 27001:2022, mencakup dimensi organisasi, manusia, fisik, dan

Penulis Korespondensi:
Agni Artika Nawawi | agniartika09@gmail.com

teknologi, sekaligus memetakan kendala yang dihadapi dan menyusun rekomendasi perbaikannya. Pendekatan yang digunakan adalah kualitatif dengan desain studi kasus. Lima informan dilibatkan dalam penelitian ini, yaitu Kepala Rekam Medis, dua staf Rekam Medis, Kepala IT, dan satu staf IT, yang seluruhnya dipilih melalui teknik purposive sampling. Data dihimpun melalui wawancara mendalam, observasi lapangan, dan telaah dokumen, kemudian diolah dengan model analisis interaktif Miles, Huberman, dan Saldãna yang mencakup tahap kondensasi data, penyajian data, hingga penarikan kesimpulan. Temuan penelitian memperlihatkan bahwa RSIJ Cempaka Putih sudah menjalankan sejumlah kontrol keamanan informasi, antara lain kebijakan dan SOP keamanan, pengaturan hak akses pengguna, prosedur *downtime*, pengamanan ruang server berbasis *fingerprint*, serta backup data otomatis setiap hari. Meski demikian, masih dijumpai sejumlah kendala, seperti minimnya kesadaran keamanan informasi pada sebagian pengguna, praktik berbagi akun, fitur audit trail yang belum diterapkan sepenuhnya, ketiadaan *privacy* screen di area pelayanan, serta cakupan CCTV yang masih terbatas. Secara keseluruhan, penerapan keamanan data pasien di rumah sakit ini sudah berjalan cukup memadai, namun tetap memerlukan penguatan pada aspek kesadaran pengguna, kepatuhan terhadap kebijakan, serta kontrol keamanan fisik dan teknologi agar semakin selaras dengan ISO/IEC 27001:2022.

Kata Kunci: Keamanan Data Pasien, Rekam Medis Elektronik, Rumah Sakit, Sistem Informasi Kesehatan, ISO/IEC 27001:2022.

PENDAHULUAN

Sebagai institusi pelayanan kesehatan, rumah sakit bertugas menyelenggarakan layanan kesehatan perorangan secara menyeluruh, meliputi rawat inap, rawat jalan, hingga gawat darurat (Kemenkes, 2020). Kemajuan teknologi informasi turut mendorong rumah sakit beralih ke Rekam Medis Elektronik (RME), yakni catatan elektronik yang berisi identitas pasien, hasil pemeriksaan, riwayat pengobatan, tindakan medis, serta layanan kesehatan yang diterima pasien. Ketentuan yang berlaku mengharuskan RME memenuhi prinsip kerahasiaan, integritas, dan ketersediaan *(Confidentiality, Integrity, Availability)* sekaligus mendukung terwujudnya interoperabilitas data kesehatan secara nasional (Kemenkes, 2022).

Keamanan data kesehatan merupakan serangkaian upaya untuk melindungi informasi pasien baik yang disimpan, diproses, maupun ditransmisikan secara digital agar tetap rahasia, utuh, dan tersedia. Di era digital, data pasien semakin rentan terhadap akses tidak sah, kebocoran, manipulasi, maupun serangan siber, sehingga keamanan data menekankan penerapan prinsip CIA disertai teknik pengamanan seperti enkripsi, autentikasi, dan audit sistem (Widiyanto, 2025). Standar internasional ISO/IEC 27001 menyediakan kerangka kerja bagi organisasi dalam membangun serta mengelola Sistem Manajemen Keamanan Informasi (SMKI), melalui tahapan identifikasi risiko, penetapan kontrol keamanan, hingga pemantauan dan evaluasi berkelanjutan yang mengacu pada siklus *Plan-Do-Check-Act* (Jauhary et al., 2022), dengan ruang lingkup kontrol yang mencakup keamanan informasi, keamanan siber, dan perlindungan privasi ((International Organization for Standardization, 2022). Penerapan ISO 27001 terbukti membantu organisasi mengidentifikasi dan mengendalikan risiko pada aset teknologi informasi, mempercepat penanganan insiden, serta mendukung kepatuhan terhadap regulasi (Ananda et al., 2024).

Sejumlah kajian terdahulu memperlihatkan bahwa pelaksanaan keamanan informasi di lingkungan rumah sakit belum sepenuhnya bebas kendala. Penelitian di RS Khusus Mata Purwokerto menemukan adanya risiko kehilangan dan manipulasi data

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

sehingga diperlukan audit keamanan berbasis ISO 27001 (Akmal et al., 2025). Penelitian pada RSUD Dr. R. Sosodoro Djatikoesoemo Bojonegoro menunjukkan tingkat kematangan keamanan informasi yang diukur melalui Indeks KAMI ternyata masih berada pada kategori tidak layak dan belum memenuhi standar minimum ISO 27001:2013 (Maraqonitatilla, 2024). Sementara itu, penelitian pada RSUD Idaman Banjarbaru menunjukkan bahwa penerapan ISO/IEC 27001 telah dilakukan melalui SIMRS Khanza, kontrol akses, enkripsi, *firewall*, serta monitoring harian, namun masih terkendala pada ketiadaan fitur *automatic log-off* dan kedisiplinan petugas dalam mengelola hak akses (Putri et al., 2024).

Sebagai rumah sakit tipe B, Rumah Sakit Islam Jakarta (RSIJ) Cempaka Putih telah menerapkan RME secara penuh sejak 1 November 2024 menggunakan SIMRS Teramedic yang terintegrasi. Rumah sakit ini pernah mengalami insiden *ransomware* pada tahun 2022 yang menyebabkan sebagian data pada unit *Casemix* dan Rekam Medis terkunci dan tidak dapat diakses kembali. Pengelolaan keamanan informasi saat ini masih mengacu pada standar internal (SNARS) dan belum sepenuhnya mengadopsi ISO/IEC 27001:2022, sehingga kebijakan keamanan dalam SPO belum mengatur pengendalian keamanan siber secara komprehensif. Kendala stabilitas jaringan serta efektivitas kebijakan pembaruan password yang belum dievaluasi secara menyeluruh menjadi aspek yang perlu dikaji lebih lanjut.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis penerapan keamanan data pasien pada Sistem Rekam Medis Elektronik di RSIJ Cempaka Putih berdasarkan kontrol ISO/IEC 27001:2022 pada aspek organisasi, orang, fisik, dan teknologi, sekaligus mengidentifikasi kendala penerapan yang terjadi serta merumuskan rekomendasi perbaikan strategis guna memperkuat tata kelola keamanan data pasien.

METODE

Studi ini dirancang dengan metode kualitatif melalui desain studi kasus, dengan tujuan menggali secara mendalam penerapan keamanan data pasien pada Sistem Rekam Medis Elektronik (RME) di RSIJ Cempaka Putih mengacu pada standar ISO/IEC 27001:2022. Pengambilan data berlangsung di RSIJ Cempaka Putih sepanjang periode Desember 2025 hingga Mei 2026. Sebanyak lima informan dilibatkan melalui teknik purposive sampling, yakni Kepala Rekam Medis, dua staf Rekam Medis, Kepala IT, dan staf IT, yang masing-masing memiliki pengetahuan, kewenangan, dan keterlibatan langsung dalam pengelolaan keamanan RME. Penentuan jumlah informan didasarkan pada prinsip kecukupan data (data sufficiency), yakni ketika informasi yang terkumpul sudah mampu menjawab tujuan penelitian dan pola temuan mulai menunjukkan pengulangan.

Data dikumpulkan dengan tiga cara, yaitu wawancara mendalam *(in-depth interview)* yang berpedoman pada panduan wawancara semi-terstruktur hasil pengembangan dari kontrol ISO/IEC 27001:2022, kemudian observasi lapangan *(field observation)* atas kondisi fisik ruang server dan area pelayanan, serta telaah dokumen yang meliputi SOP keamanan informasi dan formulir hak akses pengguna. Data yang terkumpul kemudian dianalisis menggunakan model interaktif Miles, Huberman, dan Saldãna, mencakup tahap kondensasi data, penyajian data, hingga penarikan kesimpulan. Pengkodean dilakukan secara deduktif dengan merujuk pada empat tema kontrol ISO/IEC 27001:2022, yakni pengendalian organisasi (kontrol 5.1, 5.15, 5.30), pengendalian orang (kontrol 6.3), pengendalian fisik (kontrol 7.2, 7.4), dan pengendalian teknologi (kontrol 8.7, 8.13, 8.15).

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Tabel 1. Informan Penelitian

No	Informan	Jumlah
1	Kepala Rekam Medis	1
2	Staf Rekam Medis	2
3	Kepala IT	1
4	Staf IT	1
	Jumlah Informan	5

HASIL

Aspek Organisasi *(Organizational Controls)*

Hasil wawancara dan telaah dokumen menunjukkan bahwa RSIJ Cempaka Putih telah memiliki SOP keamanan informasi sesuai kontrol 5.1 *(Information Security Policies)*, meskipun sosialisasinya kepada seluruh staf belum merata karena keterbatasan waktu dan pola kerja shift. Pada kontrol 5.15 *(Access Control),* setiap pengguna telah memiliki akun individual dengan pembatasan hak akses berdasarkan peran *(role based access)* serta fitur auto-logout setelah 10 menit tidak aktif, dan akun akan terkunci setelah tiga kali kesalahan password. Meskipun demikian, masih ditemukan praktik peminjaman akun kepada mahasiswa praktik pada kondisi tertentu, serta perbedaan pemahaman staf mengenai kebijakan pergantian password yang seharusnya dilakukan setiap 3–6 bulan. Pada kontrol 5.30 *(ICT Readiness for Business Continuity)*, rumah sakit telah memiliki prosedur downtime manual selama 30 menit untuk menjaga keberlangsungan pelayanan ketika terjadi gangguan sistem, yang umumnya disebabkan oleh faktor eksternal seperti koneksi internet dan layanan BPJS, bukan oleh insiden keamanan siber.

Aspek Orang *(People Controls)*

Pada kontrol 6.3 *(Information Security Awareness, Education and Training),* ditemukan kesenjangan kesadaran keamanan informasi, khususnya pada staf dengan usia lebih senior yang belum memahami ketentuan larangan penggunaan perangkat eksternal seperti flashdisk atau charger pada komputer rumah sakit. Kondisi ini mengindikasikan bahwa program edukasi dan pelatihan keamanan informasi belum menjangkau seluruh pengguna secara merata, sehingga perilaku sebagian staf belum sepenuhnya sejalan dengan kebijakan keamanan yang telah ditetapkan oleh manajemen.

Aspek Fisik *(Physical Controls)*

Pada kontrol 7.2 *(Physical Entry Controls)*, ruang server dilindungi dengan akses fingerprint dan pencatatan log keluar-masuk petugas, sedangkan posisi monitor pada area pelayanan telah diatur agar tidak terlihat langsung oleh pasien meskipun belum dilengkapi privacy screen. Area nurse station teridentifikasi sebagai titik rawan karena sifatnya yang terbuka. Pada kontrol 7.4 *(Physical Security Monitoring)*, pemantauan lingkungan dilakukan melalui detektor asap dan suhu, namun CCTV hanya terpasang di luar pintu ruang server sehingga aktivitas di dalam ruangan belum dapat dipantau secara visual.

Aspek Teknologi *(Technological Controls)*

Pada kontrol 8.13 *(Information Backup)*, backup data dilakukan secara otomatis setiap hari dan disimpan secara paralel pada lokasi berbeda *(off-site)*, dengan hasil uji restore yang menunjukkan tingkat keberhasilan 100%. Pada kontrol 8.15 *(Logging)*,

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

sistem baru mencatat aktivitas pengguna dalam bentuk log akses, sedangkan fitur audit trail yang lebih rinci belum diterapkan secara penuh. Pada kontrol 8.7 *(Protection Against Malware),* penggunaan flashdisk pada unit pelayanan telah dibatasi oleh pihak IT dan dilengkapi *firewall* serta antivirus berlisensi, tetapi sebagian staf mengaku belum mengetahui adanya kebijakan pembatasan tersebut sehingga penggunaan perangkat eksternal masih berpotensi terjadi pada kondisi tertentu.

Tabel 2. Gap Analysis Keamanan Data Pasien berdasarkan ISO/IEC 27001:2022

Kontrol ISO 27001	Harapan/Kebijakan	Temuan Lapangan	Identifikasi Gap
5.15 *Access Control (Password)*	Password wajib diganti berkala dan sistem mendukung forced password change.	Kebijakan pergantian password 3–6 bulan belum diketahui merata oleh staf; sistem belum memaksa perubahan otomatis.	Kesenjangan antara kebijakan manajemen dan implementasi teknis serta sosialisasi kepada pengguna.
5.15 *Access Control* (Akun)	Setiap pengguna memiliki akun pribadi dan dilarang berbagi akun.	Masih ditemukan praktik peminjaman akun kepada mahasiswa pada kondisi tertentu.	Kepatuhan pengguna terhadap kebijakan kontrol akses belum optimal.
6.3 *Security Awareness*	Seluruh pengguna memahami kebijakan keamanan informasi secara merata.	Sebagian staf belum mengetahui ketentuan penggunaan perangkat eksternal.	Kesadaran keamanan informasi belum merata pada seluruh pengguna.
7.2 *Physical Entry Controls*	Data pasien terlindungi dari pengamatan pihak yang tidak berwenang.	Area nurse station terbuka; monitor belum menggunakan privacy screen.	Pengamanan visual terhadap data pasien belum optimal.
7.4 *Physical Security Monitoring*	Area kritis dipantau CCTV dan perangkat pemantauan lingkungan.	CCTV hanya berada di luar ruang server.	Pemantauan aktivitas di dalam ruang server belum optimal.
8.15 *Logging (Audit Trail)*	Sistem mencatat seluruh aktivitas pengguna secara rinci.	Sistem baru mencatat log akses/login secara terbatas.	Sistem belum memiliki fitur audit yang mampu melacak aktivitas mendalam.

PEMBAHASAN

Aspek Organisasi berdasarkan ISO/IEC 27001:2022

Pelaksanaan kontrol organisasi di RSIJ Cempaka Putih memperlihatkan memiliki fondasi pengelolaan keamanan informasi, yang terlihat dari kebijakan keamanan, pengaturan hak akses berbasis peran, serta prosedur *downtime* sebagai langkah antisipatif ketika sistem mengalami gangguan. Keberadaan berbagai kontrol tersebut mengindikasikan upaya organisasi dalam menerapkan tata kelola keamanan informasi

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

yang selaras dengan ISO/IEC 27001:2022. Dari segi keamanan informasi, penerapan akun individual disertai pembatasan hak akses turut berkontribusi menjaga kerahasiaan data pasien, sebab setiap pengguna hanya dapat mengakses informasi sesuai kewenangan yang dimilikinya.

Meskipun demikian, masih ditemukannya praktik peminjaman akun dan belum meratanya pemahaman mengenai kebijakan pergantian *password* menunjukkan bahwa implementasi kebijakan belum sepenuhnya berjalan efektif. Kondisi ini dapat mengurangi akuntabilitas pengguna karena aktivitas dalam sistem tidak selalu dapat ditelusuri kepada pemilik akun yang sebenarnya. Temuan penelitian ini sejalan dengan penelitian oleh (Putri et al., 2024) yang menyatakan bahwa keberhasilan implementasi keamanan informasi dipengaruhi oleh kebijakan organisasi, pengelolaan akses, dan kepatuhan pengguna terhadap aturan yang berlaku. Penelitian oleh (Ardianto & Nurjanah, 2024) juga menunjukkan bahwa keamanan data pasien pada RME telah didukung oleh penggunaan *username* dan *password*, namun masih ditemukan kelemahan berupa belum dilaksanakannya pergantian password secara berkala.

Aspek Orang berdasarkan ISO/IEC 27001:2022

Keamanan informasi sangat dipengaruhi oleh perilaku pengguna sistem. Perbedaan tingkat pemahaman staf terhadap kebijakan keamanan, khususnya mengenai penggunaan perangkat eksternal, menunjukkan bahwa peningkatan kesadaran keamanan informasi masih menjadi kebutuhan. Kondisi tersebut mengindikasikan bahwa pelatihan yang telah dilakukan belum sepenuhnya menjangkau seluruh pengguna, terutama bagi staf yang telah lama bekerja dan memiliki kebiasaan penggunaan perangkat yang berbeda..

Temuan ini sejalan dengan penelitian (Setyaningrum & Ricky, 2025) serta (Izzani et al., 2026) yang menjelaskan bahwa faktor manusia merupakan salah satu penyebab utama terjadinya insiden keamanan informasi di fasilitas pelayanan kesehatan. Rendahnya kesadaran pengguna dapat meningkatkan risiko akses yang tidak sesuai prosedur maupun kebocoran data pasien. Oleh karena itu, pelatihan dan sosialisasi keamanan informasi perlu dilakukan secara berkelanjutan agar seluruh pengguna memiliki pemahaman yang sama terhadap kebijakan yang berlaku.

Aspek Fisik berdasarkan ISO/IEC 27001:2022

Pengendalian keamanan fisik di RSIJ Cempaka Putih telah diterapkan melalui pembatasan akses ke ruang server menggunakan *fingerprint* serta pencatatan log akses petugas. Pengamanan tersebut menunjukkan adanya upaya untuk melindungi aset informasi dari akses fisik oleh pihak yang tidak berwenang. Selain itu, keberadaan detektor asap dan pemantauan kondisi ruang server juga menjadi bagian penting dalam menjaga keberlangsungan operasional sistem.

Namun, masih terdapat beberapa aspek yang perlu ditingkatkan, yaitu belum tersedianya *privacy screen* pada monitor di area pelayanan dan terbatasnya cakupan CCTV di ruang server. Kondisi tersebut masih membuka peluang terjadinya pengungkapan informasi kepada pihak yang tidak berkepentingan maupun keterbatasan dalam pemantauan aktivitas pada area kritis. Hasil ini mendukung penelitian (Akmal et al., 2025) dan (Rani & Widyaningrum, 2025) yang menekankan bahwa pengamanan fisik perlu dilakukan secara menyeluruh, tidak hanya pada ruang server tetapi juga pada area pelayanan yang berhubungan langsung dengan data pasien.

Aspek Teknologi berdasarkan ISO/IEC 27001:2022

Dari aspek teknologi, rumah sakit telah menerapkan berbagai pengendalian seperti penggunaan *firewall*, antivirus berlisensi, serta mekanisme *backup* data harian yang

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

disimpan pada lokasi berbeda. Pengendalian tersebut menunjukkan adanya upaya untuk menjaga keberlangsungan layanan dan meminimalkan risiko kehilangan data apabila terjadi gangguan sistem. Penerapan *backup* yang disertai uji *restore* secara berkala juga menjadi indikator bahwa mekanisme pemulihan data telah berjalan dengan baik.

Di sisi lain, fitur *audit trail* yang masih terbatas menunjukkan bahwa kemampuan sistem dalam merekam aktivitas pengguna belum optimal. Audit trail merupakan komponen penting dalam mendukung pelacakan aktivitas pengguna dan proses investigasi apabila terjadi insiden keamanan informasi. Hal ini sejalan dengan (Dewi & Ricky, 2025) yang menegaskan bahwa pencatatan aktivitas pengguna secara rinci merupakan komponen penting dalam pengamanan sistem informasi kesehatan. Karenanya,, pengembangan fitur audit trail perlu menjadi prioritas agar pengawasan terhadap penggunaan sistem dapat dilakukan secara lebih efektif.

Kendala dan Rekomendasi Perbaikan

Kendala penerapan keamanan data pasien pada sistem RME di RSIJ Cempaka Putih bersifat teknis dan non-teknis. Kendala teknis meliputi keterbatasan fitur audit trail, belum tersedianya privacy screen, keterbatasan cakupan CCTV ruang server, serta gangguan sistem yang dipengaruhi layanan eksternal seperti BPJS dan jaringan internet. Kendala non-teknis meliputi rendahnya kesadaran keamanan informasi, ketidaktahuan sebagian staf terhadap kebijakan keamanan, serta praktik peminjaman akun pada kondisi tertentu. Temuan ini diperkuat oleh (Ramadhan et al., 2025) yang menegaskan bahwa peningkatan keamanan informasi tidak hanya mengandalkan penerapan teknologi semata, melainkan harus disertai penguatan kebijakan, manajemen risiko, dan strategi keamanan informasi yang terintegrasi pada seluruh komponen organisasi. Hal ini sejalan dengan (Sinaga & Frangky, 2024) yang menyatakan bahwa penerapan ISO/IEC 27001:2022 kerap terkendala oleh keterbatasan sumber daya, kompetensi SDM, dan dukungan organisasi, sehingga komitmen manajemen menjadi kunci utama keberhasilan tata kelola keamanan informasi.

Rekomendasi perbaikan yang dapat diberikan meliputi peningkatan sosialisasi kebijakan keamanan informasi dan evaluasi kepatuhan pengguna secara berkala, penerapan *forced password change*, penyediaan akun akses khusus bagi mahasiswa praktik, pelatihan keamanan informasi secara rutin, pemasangan *privacy screen* pada area pelayanan, perluasan cakupan pemantauan CCTV pada area kritis, pengembangan fitur audit trail yang lebih komprehensif, penguatan pengendalian penggunaan perangkat eksternal, serta evaluasi berkala terhadap mekanisme backup dan *restore* data guna meningkatkan kerahasiaan, integritas, dan ketersediaan data pasien sesuai prinsip CIA Triad dan ISO/IEC 27001:2022.

KESIMPULAN DAN SARAN

Penerapan keamanan data pasien pada Sistem Rekam Medis Elektronik di RSIJ Cempaka Putih berdasarkan ISO/IEC 27001:2022 secara umum telah berjalan cukup baik pada aspek organisasi, orang, fisik, dan teknologi, ditandai dengan tersedianya kebijakan dan SOP keamanan informasi, pengaturan hak akses berbasis peran, prosedur *downtime*, pengamanan ruang server menggunakan *fingerprint*, serta backup data otomatis harian dengan hasil uji *restore* yang selalu berhasil. Meskipun demikian, sebagian besar kesenjangan yang ditemukan tidak disebabkan oleh ketiadaan kebijakan, melainkan oleh implementasi, sosialisasi, dan kepatuhan pengguna, seperti praktik peminjaman akun, rendahnya kesadaran keamanan informasi pada sebagian staf, belum tersedianya *privacy screen* pada area pelayanan, keterbatasan cakupan pemantauan CCTV di ruang server, serta belum optimalnya penerapan fitur audit trail. Kondisi ini menunjukkan bahwa

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

keberhasilan penerapan keamanan informasi tidak cukup hanya bergantung pada penyediaan teknologi dan regulasi, tetapi juga memerlukan komitmen organisasi serta partisipasi aktif seluruh pengguna sistem dalam menjaga kerahasiaan, integritas, dan ketersediaan data pasien.

Berdasarkan simpulan tersebut, RSIJ Cempaka Putih disarankan untuk meningkatkan efektivitas sosialisasi dan evaluasi kepatuhan kebijakan keamanan informasi secara berkala, menerapkan mekanisme pergantian password otomatis serta menyediakan akun akses khusus bagi mahasiswa praktik guna mengurangi praktik peminjaman akun, menyelenggarakan pelatihan dan peningkatan kesadaran keamanan informasi secara rutin bagi seluruh pengguna, memperkuat pengamanan fisik melalui pemasangan *privacy screen* dan evaluasi cakupan pemantauan CCTV pada area kritis, serta mengembangkan fitur audit trail yang lebih komprehensif disertai penguatan pengendalian penggunaan perangkat eksternal dan evaluasi berkala terhadap mekanisme backup dan *restore* data. Upaya tersebut diharapkan dapat memperkuat tata kelola keamanan data pasien di RSIJ Cempaka Putih agar semakin sesuai dengan prinsip CIA Triad dan standar ISO/IEC 27001:2022.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Fakultas Ilmu-Ilmu Kesehatan Universitas Esa Unggul, Program Studi Rekam Medis dan Informasi Kesehatan, serta manajemen dan seluruh informan di RSIJ Cempaka Putih yang telah memberikan izin, dukungan, dan waktu selama proses pengumpulan data penelitian ini.

DAFTAR PUSTAKA

Akmal, R. N., Susilo, D. D., & Rouf, E. H. (2025). *Evaluasi Keamanan Sistem Informasi Rumah Sakit : Metode Pengujian ISO 27001 di RS Khusus Mata Purwokerto*. *6*(1), 560–569.

Ananda, N. R., Daffa, T., Salsabila, P., Nabila, A. F., Iqnatia, N., Farrel, E. R., Fitrani, L. D., Puspitaningrum, A. C., Informasi, S., Teknik, F., Hayam, U., Perbanas, W., Sakit, R., & Mode, F. (2024). *Penilaian Risiko Menggunakan Metode Analisa Failure Mode And Effects Analysis(FMEA) Dengan Standar ISO 27001 Pada Rumah Sakit*. *16*(2), 275–283.

Ardianto, E. T., & Nurjanah, L. (2024). *Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X*. *3*(2), 18–30.

Dewi, N., & Ricky, A. V. (2025). *Analisis Penerapan Audit Trail Pada Rekam Medis Elektronik Di Rumah Sakit X Jawa Tengah*. *9*(8), 4228–4236.

International Organization for Standardization. (2022). *Keamanan informasi, keamanan siber dan perlindungan privasi — Sistem manajemen keamanan informasi — Persyaratan* (Vol. 2022). https://ilide.info/doc-viewer-v2

Izzani, M., Nellatul, N., Ismatul, A., & Hamdani, A. (2026). *Evaluation of the Implementation of Information Security at SIAKAD Ibrahimy University Based on ISO / IEC 27001 : 2022*. *5*(1), 175–185. https://doi.org/https://doi.org/10.51903/d3bktm29

Jauhary, H., Pratiwi, G. E., Salim, A. Z., & Martin, T. (2022). *Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi : Literatur Review*. *14*(1). https://doi.org/10.35194/mji.v%vi%i.1581

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Kemenkes. (2020). *Peraturan Menteri Kesehatan Republik Iindonesia Nomor 3 Tahun 2020*. *3*, 1–80.

Kemenkes. (2022). *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis* (pp. 1–20).

Maraqonitatilla, G. S. P. (2024). *Analisis Tingkat Keamanan Informasi Pada RSUD Dr . R . Sosodoro Djatikoesoemo Bojonegoro*. *05*(02), 66–72. https://doi.org/https://doi.org/10.26740/jeisbi.v5i2.59469

Peraturan Pemerintah. (2021). *Peraturan Pemerintah Nomor 47 Tahun 2021 tentang Penyelenggaraan Bidang Perumahsakitan*. *086146*.

Putri, R., Khairunnisa, & Apriyanti, F. (2024). *Tinjauan Keamanan Informasi Rekam Medis Elektronik Melalui Iso 27001 Di Instalasi Rawat Jalan Rumah Sakit Daerah Idaman Banjarbaru*. *2*, 128–133. http://repository.stikeshb.ac.id/724/%0Ahttp://repository.stikeshb.ac.id/724/3/BAB I.pdf

Ramadhan, R., Widiyasono, N., & Rahmatullah, A. (2025). *Evaluasi Keamanan Informasi Sistem Informasi Manajemen RSUD KHZ Musthafa Menggunakan Indeks KAMI 5 . 0 Berbasis ISO / IEC 27001 : 2022*. *01*, 80–86.

Rani, D. M., & Widyaningrum, B. N. (2025). *Evaluasi Keamanan Informasi Sistem Rekam Medis Elektronik di RSI Sultan Agung*. *10*(1), 52–62.

Setyaningrum, E., & Ricky, A. V. (2025). *Analisis Keamanan Data Pasien Dalam Rekam Medis Elektronik Berdasarkan CIA TRIAD Di RSUD X Jawa Tengah*. *9*, 4216–4221. https://doi.org/https://doi.org/10.31004/jn.v9i3.46352

Sinaga, R., & Frangky. (2024). *Penerapan ISO / IEC 27001 : 2022 dalam Tata Kelola Keamanan Sistem Informasi : Evaluasi Proses dan Kendala*. *18*, 46–54.

Widiyanto, W. W. (2025). *Dasar-Dasar Keamanan Data Kesehatan* (Issue May).

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)