Jurnal INFORMA Politeknik Indonusa Surakarta P-ISSN : 2442-7942, E-ISSN 2716-5051
Vol. 12 Nomor 1 Juni 2026

Analisis Keamanan Data Rekam Medis Elektronik Di Rumah Sakit X Berdasarkan Keamanan Informasi Kesehatan ISO 27001:2022

Rani Ardi Indriani[1)], Sri Wulandari[2)], Frestiany Regina Putri[3)]

[1,2,3]Manajemen Informasi Kesehatan, Politeknik Indonusa Surakarta, Indonesia
[1,2,3] JL. KH. Samanhudi No.31, Bumi Laweyan, Surakarta
[1]f22060@poltekindonusa.ac.id, [2]sriwulandari@poltekindonusa.ac.id,
[3]frestiany.putri@poltekindonusa.ac.id

Abstrak

Pemanfaatan Rekam Medis Elektronik (RME) berkontribusi terhadap peningkatan efektivitas dan efisiensi pelayanan kesehatan, namun di sisi lain menimbulkan tantangan dalam menjaga keamanan informasi pasien yang bersifat sensitif dan rahasia. Penelitian ini bertujuan untuk mengevaluasi keamanan data RME di Rumah Sakit X berdasarkan kerangka kerja ISO/IEC 27001:2022. Penelitian menggunakan pendekatan kualitatif deskriptif dengan teknik pengumpulan data berupa wawancara mendalam dan telaah dokumen. Analisis dilakukan terhadap enam aspek keamanan informasi, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), autentikasi (*authentication*), pengendalian akses (*access control*), dan non-penyangkalan (*non-repudiation*). Hasil penelitian menunjukkan bahwa perlindungan kerahasiaan data telah didukung oleh penerapan enkripsi, *firewall*, dan pembatasan hak akses pengguna. Integritas data dijaga melalui penggunaan template pada SIMRS, audit log, serta tanda tangan digital internal. Ketersediaan data didukung oleh sistem pencadangan otomatis dan penggunaan dua penyedia layanan internet, meskipun lokasi penyimpanan data cadangan masih berada pada area yang sama. Mekanisme autentikasi telah memanfaatkan *username* dan *password*, namun belum didukung oleh *Multi-Factor Authentication* (MFA). Pengendalian akses telah menerapkan prinsip *Role-Based Access Control* (RBAC), sedangkan aspek nir-sangkal didukung oleh audit log dan pelacakan aktivitas pengguna. Secara keseluruhan, keamanan data RME telah diterapkan dengan cukup baik, tetapi masih diperlukan optimalisasi pada mekanisme autentikasi dan pengelolaan strategi pencadangan data.

Kata kunci: Rekam Medis Elektronik, Keamanan Informasi, ISO/IEC 27001:2022, Rumah Sakit, Keamanan Data.

Abstract

The adoption of Electronic Medical Records (EMR) has enhanced the effectiveness and efficiency of healthcare services; however, it also presents challenges in safeguarding sensitive and confidential patient information. This study aimed to evaluate the security of EMR data at Indriati Hospital Solo Baru using the ISO/IEC 27001:2022 framework. A descriptive qualitative approach was employed, with data collected through in-depth interviews and document reviews. The participants consisted of the Information Technology Manager, Head of the Medical Records Unit, Information Technology staff, and medical records personnel. The analysis focused on six information security domains: confidentiality, integrity, availability, authentication, access control, and non-repudiation. The findings indicate that data confidentiality is protected through encryption, firewall implementation, and user access restrictions. Data integrity is maintained through the use of Hospital Information System templates, audit logs, and internal digital signatures. Data availability is supported by automated backup systems and dual internet service providers, although backup storage remains located within the same physical environment. Authentication mechanisms rely on usernames and passwords, without the implementation of Multi-Factor Authentication (MFA). Access management follows the Role-Based Access Control (RBAC) model, while non-repudiation is supported through audit logs and user activity tracking. Overall, EMR data security has been implemented adequately; however, improvements are still required in authentication mechanisms and backup management strategies to strengthen information security resilience.

Keywords: Electronic Medical Records, Information Security, ISO/IEC 27001:2022, Hospital, Data Security.

1. PENDAHULUAN

Seiring meningkatnya penggunaan RME di Indonesia, maka juga meningkatkan potensi risiko keamanan informasi, seperti peretasan dan serangan ransomware, sehingga diperlukan penerapan pengamanan kuat yang mencakup enkripsi, autentikasi, serta kepatuhan terhadap regulasi keamanan data. Rumah Sakit X turut menghadapi ancaman tersebut pada tahun 2022, yang ditandai dengan adanya insiden serangan siber berupa upaya peretasan yang mengakibatkan hilangnya sebagian data. Meskipun data berhasil dipulihkan oleh tim teknologi informasi, kejadian ini menjadi peringatan serius bagi manajemen terkait penguatan sistem keamanan informasi. Apabila insiden serupa kembali terjadi tanpa mitigasi yang memadai, dampak yang ditimbulkan berpotensi merugikan secara signifikan.

Berdasarkan studi pendahuluan, ditemukan sejumlah kendala dalam praktik keamanan sistem, antara lain masih adanya pengguna yang tidak melakukan pembaruan kata sandi (*password*) secara berkala dan tidak keluar (*logout*) dari sistem setelah penggunaan. Permasalahan tersebut tidak semata-mata disebabkan oleh kelalaian individu, melainkan mencerminkan rendahnya tingkat kesadaran keamanan (*security awareness*) serta belum tersedianya mekanisme sistem yang bersifat mengikat untuk memastikan kepatuhan terhadap protokol keamanan. Standar pengamanan sistem yang diterapkan oleh unit IT saat ini masih terbatas pada SPO dan kebijakan internal rumah sakit, sehingga dinilai belum cukup kuat dalam mendukung pengelolaan keamanan data.

Selain itu, infrastruktur pencadangan data masih bergantung pada satu server yang terpusat dan belum dilengkapi dengan server cadangan tambahan sebagai lapisan pengamanan. Keterbatasan anggaran serta prioritas pengembangan fasilitas fisik sering menjadi kendala dalam penguatan infrastruktur teknologi informasi. Di sisi lain, belum diterapkannya audit internal pada Sistem Informasi Manajemen Rumah Sakit (SIMRS) berpotensi menimbulkan lemahnya pengendalian keamanan akibat tidak adanya mekanisme evaluasi dan pemantauan yang berkelanjutan. Kondisi ini meningkatkan risiko terjadinya kebocoran maupun kehilangan data serta kerentanan terhadap gangguan sistem yang dapat mengancam ketersediaan dan integritas data pasien.

2. TINJAUAN PUSTAKA

2.1 Rumah Sakit

Rumah sakit didefinisikan sebagai institusi pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara menyeluruh, mencakup pelayanan rawat inap, rawat jalan, serta gawat darurat (Permenkes, 2020). Selain menjalankan fungsi pelayanan medis, rumah sakit juga memiliki kewajiban dalam pengelolaan dan penyelenggaraan rekam medis sesuai dengan peraturan perundang-undangan yang berlaku.

2.2 Keamanan Informasi

Keamanan informasi merupakan bidang keilmuan yang berfokus pada upaya perlindungan informasi dari berbagai ancaman yang dapat menyebabkan kerusakan, perubahan, maupun akses tanpa otorisasi. Dalam ranah teknologi informasi, keamanan informasi mencakup penerapan kebijakan, prosedur, strategi, serta pemanfaatan teknologi yang dirancang untuk menjamin terjaganya kerahasiaan, integritas, dan ketersediaan data yang diproses, disimpan, maupun ditransmisikan melalui suatu sistem. Konsep keamanan informasi tidak hanya terbatas pada perlindungan data digital, tetapi juga mencakup pengamanan informasi dalam bentuk fisik dan aset intelektual yang memiliki nilai strategis bagi organisasi maupun individu (Agreindra et al., 2024).

2.3 Rekam Medis Elektronik

Rekam Medis Elektronik adalah catatan kesehatan berbasis elektronik yang memuat informasi klinis pasien, termasuk riwayat penyakit, pengobatan, serta tindakan medis yang diberikan. Data tersebut disusun secara terstruktur, dikelola secara sistematis, dan disahkan melalui mekanisme tanda tangan elektronik. Selain itu, penyelenggaraan Rekam Medis Elektronik wajib terintegrasi dengan platform layanan kesehatan nasional yang ditetapkan oleh Kementerian Kesehatan, yaitu platform SATU SEHAT,

sebagaimana diatur dalam Peraturan Menteri Kesehatan (Permenkes, 2022).

2.4 Standar ISO/IEC 27001:2022

ISO/IEC 27001:2022 adalah standar yang mengatur Sistem Manajemen Keamanan Informasi (*Information Security Management System*/ISMS) yang menyediakan kerangka kerja dalam melakukan evaluasi, penerapan, serta pemeliharaan keamanan informasi berdasarkan praktik terbaik (*best practices*) pengelolaan keamanan informasi dalam suatu organisasi (Jauhary et al., 2022). Implementasi standar ini dapat membantu rumah sakit dalam mengelola risiko keamanan informasi secara terstruktur dan sistematis, khususnya pada pengelolaan sistem informasi rumah sakit dan penerapan Rekam Medis Elektronik (Programme, 2022).

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan desain deskriptif. Pengumpulan data dilakukan melalui teknik wawancara dan studi dokumentasi. Tujuan penelitian adalah untuk memperoleh pemahaman yang mendalam mengenai kondisi serta berbagai hambatan dalam penerapan keamanan data Rekam Medis Elektronik (RME) di Rumah Sakit X. Populasi penelitian berjumlah 51 orang yang terdiri atas petugas rekam medis dan staf teknologi informasi rumah sakit. Pemilihan subjek penelitian dilakukan dengan teknik purposive sampling, melibatkan 5 informan kunci yang memiliki keterlibatan langsung dalam pengelolaan dan pengamanan data RME, yaitu 1 Manajer Teknologi Informasi, 1 Kepala Unit Rekam Medis, 2 staf Teknologi Informasi, dan 1 staf rekam medis.

Objek penelitian adalah sistem keamanan data Rekam Medis Elektronik yang diterapkan di rumah sakit tersebut. Variabel penelitian, yaitu *Confidentiality, Integrity, Availability, Access Control, Authentication,* dan *Non-Repudiation*. Pengumpulan data dilakukan melalui wawancara mendalam untuk menggali informasi dari para informan serta studi dokumentasi. Data yang diperoleh selanjutnya dianalisis melalui tahapan reduksi data, triangulasi data, penyajian data dalam bentuk narasi deskriptif dan tabel, serta penarikan kesimpulan guna menghasilkan gambaran yang komprehensif mengenai kondisi keamanan data RME.

4. HASIL DAN PEMBAHASAN

4.1 Aspek Kerahasiaan (*Confidentiality*)

a. Aspek Kerahasiaan (*Confidentiality*) dari sisi IT

Tabel 1. Aspek *Confidentiality* IT

Pertanyaan IT	Informan 2	Informan 3
1. Bagaimana enkripsi diterapkan pada perangkat lunak dan jaringan	Dari SIMRS	Dari SIMRS
2. Bagaimana sistem mendeteksi dan menangani kebocoran data	Melalui *Fireswall*	Pembatasan hak akses di SIMRS
3. Apakah komunikasi data antara server dan klien dienkripsi	Iya, dienkripsi	Iya, melalui prosedur enkripsi
4. Bagaimana pengamanan konfigurasi jaringan dilakukan agar data tidak bocor	Melalui enkripsi serta kontrol akses	Mengontrol enkripsi
5. Apakah ada kebijakan terkait penggunaan SIMRS	Dibatasi untuk akses publiknya	Dibatasi hanya melalui WiFi karyawan
6. Bagaimana pelatihan keamanan data	Edukasi penggantian *passowrd*	Edukasi penggantian *password*

Tabel 1 memaparkan hasil wawancara yang diperoleh Informan 2 dan Informan 3 mengungkapkan bahwa mekanisme enkripsi data telah diterapkan melalui sistem SIMRS yang disediakan vendor, sedangkan proses komunikasi antara server dan klien diamankan menggunakan prosedur enkripsi tertentu. Hasil triangulasi memperkuat temuan tersebut dengan menunjukkan bahwa sistem enkripsi telah terintegrasi pada

SIMRS, termasuk pada proses pertukaran data dengan pihak eksternal seperti BPJS melalui penggunaan *Application Programming Interface* (API) yang menghubungkan aplikasi perangkat lunak untuk berkomunikasi dan saling bertukar data. Selain itu, perlindungan jaringan dilakukan melalui penerapan *Firewall*, pengendalian hak akses, serta pembatasan penggunaan SIMRS hanya pada jaringan WiFi internal karyawan. Triangulasi juga mengungkapkan adanya Standar Prosedur Operasional (SPO) terkait keamanan dan pengelolaan data, disertai kewajiban sumpah profesi bagi seluruh tenaga kerja untuk menjaga kerahasiaan informasi rumah sakit.

Hasil penelitian ini sejalan dengan temuan Wardani et al., (2024) di Rumah Sakit Islam Jakarta Sukapura yang menyatakan bahwa implementasi keamanan RME pada rumah sakit umumnya telah menerapkan pengamanan dasar berupa enkripsi dan kontrol akses, meskipun masih diperlukan penguatan pada beberapa aspek tertentu. Dalam aspek pengawasan internal, hasil triangulasi menunjukkan bahwa audit internal rutin belum dilaksanakan secara konsisten. Pengendalian kerahasiaan data masih lebih banyak bergantung pada perlindungan sistem IT dan koordinasi langsung dengan pimpinan rumah sakit.

b. Aspek Kerahasiaan (*Confidentiality*) dari sisi Rekam Medis

Tabel 2. Aspek *Confidentiality* Rekam Medis

Pertanyaan Rekam Medis	Informan 4	Informan 5
1. Bagaimana kebijakan rekam medis menjaga kerahasiaan data pasien	Pedoman dan SPO Rekam Medis	SPO Rekam Medis
2. Apakah ada pelatihan rutin	Pelatihan rutin tidak ada adanya evaluasi rutin	Pelatihan hanya ada satu kali diawal, adanya evaluasi rutin
3. Bagaimana menangani jika pasien atau keluarga meminta data RME orang lain	Melalui prosedur	Melalui prosedur RS
4. Bagaimana menjaga kerahasiaan data saat shift berganti di unit rekam medis	*Logout* sistem	*Logout* sistem saat pergantian shift
5. Pernahkah ada insiden hampir bocornya data RME, dan bagaimana penanganannya	Belum pernah	Belum pernah

Dalam tabel 2, menunjukkan hasil wawancara dengan Informan 4 dan Informan 5 mengungkapkan bahwa perlindungan kerahasiaan data pasien dilaksanakan sesuai pedoman dan SPO Rekam Medis yang berlaku. Prosedur log out sistem dilakukan setiap pergantian shift sebagai bentuk pengamanan akses, serta kedua informan menyampaikan bahwa hingga saat ini belum pernah ditemukan kasus kebocoran data pasien. Selain itu, permintaan akses rekam medis oleh pasien maupun anggota keluarga diproses sesuai ketentuan dan prosedur resmi rumah sakit.

Hasil penelitian juga menunjukkan adanya ketidakkonsistenan terkait pelaksanaan pelatihan keamanan data. Informan 4 menyatakan bahwa tidak terdapat pelatihan rutin dan hanya dilakukan evaluasi berkala, sedangkan Informan 5 menjelaskan bahwa pelatihan hanya diberikan pada awal penerapan sistem. Kondisi tersebut belum sesuai dengan prinsip *continual improvement* yang menjadi bagian penting dalam ISO 27001:2022.

4.2 Aspek Integritas (*Integrity*)

a. Aspek Integritas (*Integrity*) dari sisi IT

Tabel 3. Aspek *Integrity* IT

Pertanyaan IT	Informan 2	Informan 3
1. Bagaimana perangkat lunak memvalidasi dan menjaga keakuratan data rekam medis	*Template* SIMRS	*Template* SIMRS
2. Apakah perangkat lunak	Tanda tangan internal	Tanda tangan internal

Pertanyaan IT	Informan 2	Informan 3
menggunakan tanda tangan digital		
3. Bagaimana *update* perangkat lunak dijalankan	*Downtime* sementara	*Downtime*
4. Bagaimana *Backup* dan pemulihan dijalankan	*Backup* otomatis dan *Backup* manual	*Backup* otomatis dan *Backup* manual
5. Bagaimana perangkat lunak mengatasi konflik data yang mungkin terjadi	Dicegah melalui log di SIMRS	Melalui log SIMRS
6. Apakah ada monitoring otomatis	Tersedia fitur log aktivitas	Menggunakan log aktivitas

Merunjuk pada tabel 3, dapat dilihat hasil wawancara dengan Informan 2 dan Informan 3 memvalidasi ketepatan data dilakukan melalui penggunaan template SIMRS yang berfungsi sebagai standar pengisian informasi. Sistem juga telah dilengkapi dengan tanda tangan digital internal, mekanisme *Backup* otomatis maupun manual, serta pencatatan *log activity* guna mendeteksi dan menelusuri potensi konflik data. Hasil triangulasi memperjelas bahwa sistem memanfaatkan master data berbasis pilihan *dropdown* untuk mengurangi risiko kesalahan input, walaupun sistem belum sepenuhnya mampu mendeteksi kesalahan pemilihan data oleh pengguna. Selain itu, setiap perubahan data diwajibkan disertai berita acara yang memuat alasan perubahan dan memperoleh persetujuan dari pihak berwenang. Data yang telah tersimpan tidak dapat dihapus, melainkan hanya dapat diperbaiki dengan tetap mempertahankan riwayat perubahan, termasuk identitas pengguna yang melakukan revisi dan jenis perubahan yang dilakukan. Seluruh pembaruan maupun penambahan fitur sistem juga harus melalui prosedur pengajuan resmi sebelum diproses oleh tim IT.

Hasil penelitian ini sejalan dengan temuan Widiyanti et al., (2024) di Puskesmas Tasikmadu Karanganyar yang menunjukkan bahwa integritas data dapat terjaga karena hak edit hanya diberikan kepada pengguna sesuai kewenangannya, sedangkan penghapusan data dibatasi pada pihak tertentu yang memiliki otorisasi khusus. Kondisi serupa juga ditemukan di Rumah Sakit X, namun dengan mekanisme pengamanan tambahan berupa berita acara perubahan data yang lebih komprehensif.

b. Aspek Integritas (*Integrity*) dari sisi Rekam Medis

Tabel 4. Aspek *Integrity* Rekam Medis

Pertanyaan Rekam Medis	Informan 4	Informan 5
1. Apakah ada langkah pemeriksaan ulang data RME sebelum disimpan ke sistem elektronik	Ada	Ada
2. Apa langkah jika menemukan kesalahan data pasien setelah disimpan	Dilakukan revisi	Melakukan revisi sebelum pasien pulang
3. Bagaimana menangani duplikasi data pasien di sistem RME	Melalui pengecekan kunjungan	Pengecekan jumlah kunjungan
4. Apa fitur yang bantu cegah kesalahan input manual data RME	Ada fitur *warning*	Terdapat sistem *bridging* dan fitur *warning*
5. Apakah ada pelatihan terkait peningkatan akurasi pengisian rekam medis	Tidak ada	Tidak ada
6. Apakah ada pengalaman kesalahan pengisian data rekam medis	Pernah	Pernah

Ditinjau dari tabel 4 diatas, mengungkapkan hasil wawancara dengan Informan 4 dan Informan 5 menjelaskan bahwa terdapat prosedur pemeriksaan ulang sebelum data disimpan ke dalam sistem. Apabila ditemukan kesalahan, revisi

dilakukan sebelum pasien dipulangkan. Selain itu, identifikasi duplikasi data dilakukan melalui verifikasi jumlah kunjungan pasien, sedangkan fitur warning dan bridging dimanfaatkan untuk meminimalkan kesalahan input manual. Meskipun demikian, kedua informan menyampaikan bahwa belum tersedia pelatihan khusus yang berfokus pada peningkatan akurasi pengisian rekam medis, serta mengakui bahwa kesalahan input masih pernah terjadi dalam praktik pelayanan.

Temuan ini sejalan dengan penelitian Puteri et al., (2024) yang menyatakan bahwa sejumlah fasilitas kesehatan yang telah menerapkan autentikasi, enkripsi, dan pembatasan akses masih menghadapi risiko kesalahan maupun kebocoran data akibat lemahnya pengawasan. Kondisi tersebut menyebabkan implementasi keamanan informasi belum sepenuhnya memenuhi standar ISO 27001:2022.

4.3 Aspek ketersediaan (*Availability*)

a. Aspek Ketersediaan (*Availability*) dari sisi IT

Tabel 5. Aspek *Availability* IT

Pertanyaan IT	Informan 2	Informan 3
1. Bagaimana jaringan dijaga agar tetap stabil dan aman dari serangan	*Firewall*	*Firewall*
2. Apa mekanisme deteksi dan mitigasi serangan	*Firewall* dan memantau log	Sistem log dan *Firewall*
3. Bagaimana *Backup* data dijadwalkan dan dikelola pada sistem perangkat lunak	Dijadwalkan otomatis	Sudah otomatis
4. Apakah ada mekanisme *failover* (peralihan otomatis)	*Single* jalur	Masih satu jalur utama
5. Bagaimana pengelolaan kapasitas sistem agar tidak *overload*	Memantau server	Monitoring berkala
6. Bagaimana pengamanan fisik dan virtual perangkat jaringan	Dibatasi aksesnya	Aksesnya terbatas dan dikunci

Tabel 5 menguraikan jawaban yang diberikan oleh Informan 2 dan Informan 3 menyebutkan bahwa kestabilan jaringan dipertahankan melalui penggunaan *Firewall*, pelaksanaan *Backup* data secara terjadwal, serta pemantauan kapasitas server secara berkala. Selain itu, pengamanan fisik server dilakukan dengan membatasi akses ke ruang server hanya bagi pihak tertentu. Hasil triangulasi memberikan informasi yang lebih komprehensif, yaitu rumah sakit telah menggunakan dua penyedia layanan internet (*Internet Service Provider* atau ISP) sebagai sistem cadangan. Dengan mekanisme tersebut, apabila ISP utama mengalami gangguan, sistem akan otomatis beralih ke ISP kedua tanpa menghentikan layanan operasional. Proses *Backup* data dilaksanakan setiap hari secara otomatis dan diawasi oleh tiga personel tim *software* IT.

Rumah sakit juga telah memiliki Standar Prosedur Operasional (SPO) yang mengatur jadwal *Backup* harian dan mingguan, pemeriksaan kapasitas penyimpanan, serta prosedur otomatisasi sistem. Dalam kondisi downtime yang berlangsung lebih dari satu jam, prosedur darurat manual akan diberlakukan. Meskipun demikian, hasil triangulasi juga menunjukkan adanya kelemahan mendasar, yaitu penyimpanan data cadangan masih berada pada server dan lokasi fisik yang sama (*on-premise*). Proses pengadaan server cadangan di lokasi berbeda masih berada pada tahap pengembangan. Risiko utama yang diidentifikasi adalah potensi kehilangan data akibat kerusakan sistem atau penghapusan data secara sengaja.

Temuan tersebut sejalan dengan penelitian Luvi et al., (2025) mengenai infrastruktur RME di RSUD Kabupaten Kediri yang menunjukkan bahwa meskipun rumah sakit telah memiliki dukungan listrik cadangan berupa genset, penguatan infrastruktur jaringan dan sistem cadangan masih menjadi tantangan. Oleh sebab itu, implementasi ketentuan terkait penyimpanan

Backup di lokasi terpisah menjadi kebutuhan yang mendesak untuk dipenuhi.

b. Aspek Ketersediaan (*Availability*) dari sisi Rekam Medis

Tabel 6. Aspek *Availability* Rekam Medis

Pertanyaan Rekam Medis	Informan 4	Informan 5
1. Bagaimana mengakses RME saat sistem lambat di jam ramai dan apa dampaknya	Menunggu IT jika lama dialihkan manual, dampak hambat layanan	Hambat pelayanan, tunggu estimasi IT jika lama maka manual
2. Bagaimana jika sistem RME down dan data pasien dibutuhkan segera	Manual	Manual
3. Bagaimana *Backup* data dilakukan dari sisi staf rekam medis	Manual	Manual ke DRM
4. Bagaimana koordinasi dengan IT saat gangguan	Jika IT akan menginstruksi manual maka manual	IT akan memberikan instruksi, jika manual maka manual
5. Pernahkah data RME hilang sementara, dan bagaimana *recovery*-nya (pemulihan)	Belum pernal	Belum pernal
6. Apakah ada protokol akses manual jika sistem elektronik terganggu	Ada	Ada

Dilihat dari tabel 6, menggambarkan jawaban dari Informan 4 dan Informan 5 menjelaskan bahwa ketika sistem mengalami perlambatan atau gangguan (*down*), petugas akan berkoordinasi dengan bagian IT dan sementara waktu beralih pada pencatatan manual sesuai arahan yang diberikan. Selain itu, *Backup* data pada tingkat unit dilakukan secara manual melalui penyimpanan Dokumen Rekam Medis (DRM). Kedua informan juga menyampaikan bahwa hingga saat ini belum pernah terjadi kehilangan data sementara, serta telah tersedia prosedur akses manual yang digunakan dalam kondisi darurat. Namun demikian, mereka mengakui bahwa gangguan sistem berdampak pada terhambatnya proses pelayanan pasien.

Penelitian Septiana et al., (2025) di RSUD Patut Patuh Patju Gerung menunjukkan bahwa meskipun rumah sakit telah menerapkan *Backup* harian dan prosedur darurat, masih ditemukan kendala berupa system error dan data ganda yang memengaruhi ketersediaan data secara akurat. Temuan ini mengindikasikan bahwa keberadaan sistem *Backup* belum sepenuhnya menjamin kesinambungan akses dan konsistensi data.

4.4 Aspek Autentikasi (*Authentication*)

a. Aspek Autentikasi (*Authentication*) dari sisi IT

Tabel 7. Aspek *Authentication* IT

Pertanyaan IT	Informan 2	Informan 3
1. Bagaimana sistem mengelola proses *login* dan autentikasi pengguna	Terpusat	Terpusat
2. Apakah sistem menggunakan autentikasi multifaktor	Belum	Belum
3. Bagaimana sistem menghadapi *login* yang mencurigakan	Menggunakan fitur log	Memantau log
4. Apakah ada pelatihan dan edukasi terkait keamanan *login* bagi pengguna	Ada	Pelatihan hanya ada pada saat training
5. Bagaimana sistem menangani sesi pengguna yang tidak aktif	Dengan koordinasi HDR	Koordinasi HRD

Pertanyaan IT	Informan 2	Informan 3
6. Apakah ada mekanisme audit terhadap aktivitas autentikasi	Audit log di SIMRS dan *history*	Audit log aktivitas

Sebagaimana yang tersaji pada tabel 4.7, berikut ini merupakan hasil wawancara dengan Informan 2 dan Informan 3 menyebutkan bahwa sistem *login* pada RME dikelola secara terpusat, dilengkapi dengan audit log dan riwayat aktivitas pengguna, serta memiliki fitur pemantauan terhadap aktivitas *login* yang mencurigakan. Hasil triangulasi menunjukkan bahwa proses autentikasi masih menggunakan kombinasi username dan *password* dengan ketentuan minimal delapan karakter. Pengguna diwajibkan mengganti kata sandi bawaan saat pertama kali akun dibuat, dan sistem secara berkala memberikan pengingat untuk melakukan perubahan kata sandi melalui notifikasi otomatis. Selain itu, sistem telah menerapkan fitur auto-*logout* setelah sekitar satu jam tidak terdapat aktivitas pengguna. Pengaturan tersebut merupakan penyesuaian dari kebijakan sebelumnya yang menetapkan batas waktu 15 menit, namun dinilai terlalu singkat oleh pengguna. Pada aplikasi mobile internal yang dikembangkan rumah sakit telah diterapkan autentikasi berbasis One Time *Password* (OTP) yaitu penggunaan kata sandi sekali pakai yang berlaku hanya untuk satu sesi otentikasi, sedangkan SIMRS dari vendor belum mendukung fitur tersebut.

Hasil triangulasi juga mengungkapkan permasalahan yang cukup krusial, yaitu masih ditemukannya praktik berbagi kata sandi antarstaf serta kebiasaan tidak melakukan *logout* setelah penggunaan sistem. Penanganan terhadap kondisi ini masih berfokus pada pemberian edukasi kepada kepala unit dan staf, tanpa disertai mekanisme teknis yang mampu mencegah praktik berbagi akun secara langsung. Selain itu, pihak IT menyebutkan bahwa insiden keamanan yang paling sering terjadi berkaitan dengan human *error*, seperti lupa melakukan *logout*, penggunaan kata sandi bawaan, dan kebiasaan berbagi *password*.

Temuan ini didukung oleh penelitian Artiningsih et al., (2026) terkait implementasi fitur keamanan SIMRS di RSUD Sultan Suriansyah Kota Banjarmasin juga menemukan bahwa keterbatasan fitur *logout* otomatis menjadi salah satu kelemahan utama sistem keamanan rumah sakit. Hal ini menunjukkan bahwa permasalahan autentikasi masih menjadi tantangan umum pada berbagai fasilitas kesehatan di Indonesia.

b. Aspek Autentikasi (*Authentication*) dari sisi Rekam Medis

Tabel 8. Aspek *Authentication* Rekam Medis

Pertanyaan Rekam Medis	Informan 4	Informan 5
1. Seberapa sering ganti *password*	Rata-rata satu kali sejak sistem digunakan	Sesuai staffnya
2. Bagaimana jaga kerahasiaan *password* dari staf lain	Berprinsip pada diri sendiri	Disimpan diri sendiri
3. Apa kendala yang sering muncul saat mengakses data pasien	Koneksi jaringan	Koneksi jaringan lemot
4. Apakah hambatan tersebut berpengaruh pada pelayanan darurat rekam medis	Berpengaruh	Berpengaruh

Pada tabel 8 berikut ini disajikan data hasil wawancara dengan Informan 4 menjelaskan bahwa pergantian kata sandi umumnya hanya dilakukan satu kali sejak awal penggunaan sistem, sedangkan Informan 5 menyatakan bahwa frekuensi perubahan *password* bergantung pada kebiasaan masing-masing staf. Kerahasiaan kata sandi lebih banyak mengandalkan kesadaran individu tanpa adanya sistem yang secara teknis memaksa pengguna untuk melakukan pembaruan berkala. Selain itu, kendala jaringan yang tidak stabil disebut sebagai hambatan utama dalam mengakses data pasien dan dinilai memengaruhi kelancaran pelayanan, termasuk pada kondisi kegawatdaruratan.

Temuan tersebut sejalan dengan penelitian Ardianto et al., (2025) yang menunjukkan bahwa praktik pergantian kata

sandi secara berkala masih belum diterapkan secara optimal, meskipun kebijakan penggunaan kombinasi karakter khusus pada *password* telah diberlakukan. Kondisi ini konsisten dengan hasil penelitian di Rumah Sakit X dan memperkuat kebutuhan akan penerapan kebijakan manajemen kata sandi yang lebih ketat, terstandarisasi, dan didukung mekanisme teknis yang tidak hanya bergantung pada kesadaran pengguna.

4.5 Aspek Kontrol Akses (*Access Control*)

a. Aspek Kontrol Akses (*Access Control*) dari sisi IT

Tabel 9. Aspek *Access Control* IT

Pertanyaan IT	Informan 2	Informan 3
1. Bagaimana sistem mengatur hak akses per pengguna	Berdasarkan unit kerjanya	Berdasarkan unit kerjanya
2. Apakah ada monitoring *r e a l - t i m e* terhadap penggunaan hak akses	Jika ada pengaduan terkait terjadi masalah	Jika ada pengaduan dari *user*
3. Bagaimana penerapan prinsip *Least Privilege* (batasan akses)	Ada	Ada
4. Bagaimana penanganan akses darurat dalam situasi kritis	Diutamakan IGD	Diutamakan IGD

Tabel 9 di atas, menggambarkan hasil wawancara Informan 2 dan Informan 3 menjelaskan bahwa pengaturan hak akses pengguna pada sistem dilakukan sesuai unit kerja dengan menerapkan prinsip *Least Privilege*. Dalam kondisi darurat, sistem memberikan prioritas akses kepada Instalasi Gawat Darurat (IGD) untuk mendukung kelancaran pelayanan pasien. Hasil triangulasi menunjukkan bahwa penentuan hak akses dilakukan melalui formulir pengajuan yang diisi oleh atasan pengguna. Formulir tersebut digunakan untuk menentukan modul sistem yang dapat diakses sesuai tugas dan tanggung jawab masing-masing staf. Selain itu, penyesuaian maupun pencabutan hak akses dilakukan melalui mekanisme yang sama, baik ketika pegawai berpindah unit maupun berhenti bekerja.

Pemantauan akses dilakukan melalui penggunaan *Firewall* untuk mengawasi lalu lintas jaringan serta pemeriksaan *log activity* secara berkala guna mendeteksi potensi anomali. Namun demikian, pihak IT dan triangulasi mengakui bahwa proses monitoring masih bersifat reaktif, yaitu dilakukan setelah terdapat laporan atau keluhan dari pengguna. Hingga saat ini belum tersedia sistem pemantauan otomatis secara *real-time* yang mampu mendeteksi aktivitas mencurigakan secara berkelanjutan.

Temuan ini sejalan dengan penelitian N. Dewi & Ricky, (2025) yang dikutip dalam kajian perlindungan hak akses di RSUD Cililin, yang menyebutkan bahwa penerapan audit trail pada rekam medis elektronik di RS X Jawa Tengah belum berjalan optimal. Penelitian tersebut juga menunjukkan bahwa implementasi RBAC melalui SIMGOS telah dilakukan secara prosedural dengan mekanisme pengajuan hak akses secara tertulis dan diketahui kepala ruangan, namun pengawasan *real-tim*e masih menjadi tantangan yang belum terselesaikan.

b. Aspek Kontrol Akses (*Access Control*) dari sisi Rekam Medis

Tabel 10 Aspek *Access Control* Rekam Medis

Pertanyaan Rekam Medis	Informan 4	Informan 5
1. Apakah ada pembatasan akses berdasarkan waktu atau lokasi	Ada	Ada
2. Bagaimana pembagian level akses data RME berdasarkan jabatan staf	Sesuai *job desk*	*Job desk* staff
3. Apakah ada prosedur untuk memberikan atau mencabut hak akses staf	Ada	Ada
4. Apa pelatihan soal aturan kontrol akses di tim rekam medis	Terkait *job desk* dan evaluasi rutin	*Job desk*, sisanya evaluasi

Pertanyaan Rekam Medis	Informan 4	Informan 5
5. Menurut Anda, apa risiko jika akses RME terlalu bebas bagi staf	Penyalahgunaan dan pelepasan informasi	Penyalahgunaan data

Berikut ini tabel 10 yang memuat rangkuman hasil wawancara dengan Informan 4 dan Informan 5 menjelaskan bahwa pembatasan akses diterapkan berdasarkan waktu maupun lokasi tertentu. Pembagian tingkat akses juga disesuaikan dengan jabatan dan tugas masing-masing staf sesuai job description. Selain itu, rumah sakit telah memiliki prosedur formal terkait pemberian dan pencabutan hak akses, disertai pelatihan serta evaluasi rutin mengenai kontrol akses. Kedua informan menunjukkan pemahaman yang cukup baik terkait risiko penyalahgunaan data apabila akses diberikan secara terlalu luas.

Penelitian Mulyani et al., (2023) di RSUP Dr. Hasan Sadikin Bandung menunjukkan bahwa pemberian hak akses RME untuk kepentingan penelitian masih memiliki potensi penyalahgunaan meskipun prosedur formal telah diterapkan. Hal tersebut terjadi karena durasi akses yang diberikan terkadang melebihi kebutuhan aktual pengguna. Temuan ini menegaskan pentingnya penerapan prinsip *Least Privilege* yang tidak hanya diterapkan secara administratif dan teknis, tetapi juga dievaluasi secara berkala agar tetap sesuai dengan kebutuhan dan tanggung jawab pengguna.

4.6 Aspek Nir-Sangkal (*Non-Repudiation*)

a. Aspek Nir-Sangkal (*Non-Repudiation*) dari sisi IT

Tabel 11. Aspek *Non-Repudiation* IT

Pertanyaan IT	Informan 2	Informan 3
1. Bagaimana catatan log aktivitas pengguna disimpan dan dianalisis	Log disimpan kepala unit dan dianalisis jika ada *error*	Log disimpan dan dianalisis jika ada *error*
2. Bagaimana penyimpanan bukti otentik aktivitas pengguna	Semua terekam di SIMRS	Terekam di SIMRS
3. Apakah sistem dilengkapi dengan proteksi terhadap manipulasi log	Ya	Ya
4. Bagaimana mekanisme penanganan insiden keamanan	Otomatis akan ke blok	Otomatis ke blok
5. Apakah ada standar kepatuhan yang diikuti dalam pengelolaan log	Setiap aplikasi berbeda, namun tetap distandarkan	Log dibuat agar dapat di cek

Pada tabel 11 berikut, mengungkapkan jawaban dari Informan 2 dan Informan 3 menyimpulkan bahwa sistem telah menyimpan catatan log activity pengguna yang digunakan untuk analisis apabila terjadi kesalahan sistem maupun insiden keamanan. Seluruh aktivitas pengguna tercatat di dalam SIMRS, disertai mekanisme perlindungan terhadap manipulasi log dan fitur pemblokiran otomatis ketika terdeteksi ancaman tertentu. Hasil triangulasi memperkuat temuan tersebut dengan menunjukkan bahwa data yang telah dimasukkan ke sistem tidak dapat dihapus, melainkan hanya dapat diperbaiki dengan tetap menyimpan riwayat perubahan secara lengkap, termasuk identitas pengguna yang melakukan perubahan dan jenis data yang dimodifikasi.

Selain itu, hasil triangulasi mengungkapkan bahwa rumah sakit pernah mengalami serangan *ransomware* pada data bagian pemasaran (*marketing*). Insiden tersebut menjadi dasar bagi peningkatan edukasi keamanan informasi serta rencana pengadaan tambahan *Endpoint Security*. Triangulasi juga menyatakan bahwa Rumah Sakit X belum memperoleh sertifikasi resmi ISO 27001:2022, namun telah mulai menerapkan prinsip-prinsip keamanan informasi secara bertahap. Dalam implementasinya, tanggung jawab keamanan teknis berada pada tim IT yang terdiri dari

enam personel, sedangkan seluruh pegawai rumah sakit diwajibkan mematuhi kontrak kerahasiaan data sebagai bagian dari tanggung jawab operasional.

Temuan ini sejalan dengan penelitian N. Dewi & Ricky, (2025) terkait penerapan audit trail pada RME di RS X Jawa Tengah yang menyebutkan bahwa fitur audit trail telah tersedia, tetapi implementasinya belum optimal sehingga aspek *Non-Repudiation* belum sepenuhnya terjamin. Wardani et al., (2024) dalam penelitian di RS Islam Jakarta Sukapura juga menyatakan bahwa meskipun penggunaan username dan *password* telah diterapkan sebagai dasar identifikasi pengguna, masih terdapat kelemahan pada konsistensi penggunaan tanda tangan digital yang merupakan komponen penting dalam penerapan *Non-Repudiation*.

b. Aspek Nir-Sangkal (*Non-Repudiation*) dari sisi Rekam Medis

Tabel 12. Aspek *Non-Repudiation* Rekam Medis

Pertanyaan Rekam Medis	Informan 4	Informan 5
1. Apakah sistem RME dapat mencatat dan menyimpan bukti aktivitas staf	Ada *tracking*	Bisa, ditelusur
2. Apakah ada tanda tangan digital pada entri rekam medis elektronik	Sudah ada, namun masih terbatas	Sudah ada, namun masih terbatas
3. Bagaimana log dapat bantu selidiki kesalahan di unit rekam medis	Men-*tracking* *user* terakhir	Akan ditelusur IT akses terakhir siapa

Melihat tabel 12, menunjukkan gambaran dari hasil wawancara dengan Informan 4 dan Informan 5 menjelaskan bahwa sistem RME telah memiliki fitur *tracking* untuk menelusuri aktivitas pengguna, termasuk identifikasi staf terakhir yang mengakses atau mengubah data pasien. Penerapan tanda tangan digital juga telah dilakukan, meskipun masih terbatas dan belum mencakup seluruh jenis entri rekam medis. Selain itu, penelusuran log activity dilakukan oleh tim IT apabila ditemukan permasalahan pada data.

Penelitian Wardani et al., (2024) mengenai persiapan implementasi tanda tangan digital pada dokumen RME di RSUD dr. H. Moch Ansari Saleh Banjarmasin menyatakan bahwa keberhasilan penerapan tanda tangan digital membutuhkan dukungan infrastruktur, regulasi internal, serta pelatihan pengguna yang memadai. Temuan tersebut menunjukkan bahwa pengembangan tanda tangan digital di Rumah Sakit X tidak hanya memerlukan kesiapan teknologi, tetapi juga strategi manajemen perubahan yang terencana dan menyeluruh.

5. PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai keamanan data Rekam Medis Elektronik (RME) di Rumah Sakit X yang dianalisis menggunakan standar ISO/IEC 27001:2022, diperoleh beberapa kesimpulan sebagai berikut:

1. Kerahasiaan (*Confidentiality*) pada keamanan data rekam medis elektronik menyimpulkan bahwa enkripsi data telah terintegrasi dalam SIMRS dan didukung Firewall serta segmentasi jaringan. Namun, pelatihan keamanan informasi bagi pengguna masih terbatas sehingga tingkat *security awareness* belum optimal.
2. Integritas (*Integrity*) pada keamanan data rekam medis elektronik menyimpulkan bahwa integritas data dijaga melalui *Template* SIMRS berbasis master data, audit log perubahan, dan tanda tangan digital. Kelemahan utama adalah *Backup* yang masih tersimpan dalam satu server (*Single point of failure*) dan belum adanya pelatihan akurasi pengisian data.
3. Ketersediaan (*Availability*) pada keamanan data rekam medis elektronik menyimpulkan bahwa ketersediaan data terjaga melalui dua ISP, *Backup* otomatis terjadwal, UPS, dan prosedur downtime yang jelas. Namun, server *Backup* belum berada di lokasi fisik terpisah sehingga risiko kehilangan data akibat bencana fisik masih ada.
4. Autentikasi (*Authentication*) pada keamanan data rekam medis elektronik menyimpulkan bahwa autentikasi dikelola secara terpusat melalui SIMRS, namun *Multi-Factor Authentication* (MFA) belum diterapkan. Kebijakan

penggantian *password* tidak seragam antarunit dan praktik berbagi *password* masih ditemukan di lapangan.

5. Kontrol Akses (*Access Control*) pada keamanan data rekam medis elektronik menyimpulkan bahwa *Role-Based Access Control* (RBAC) dan prinsip *Least Privilege* telah diterapkan dengan prosedur pemberian dan pencabutan hak akses yang formal. Kelemahan utama adalah monitoring hak akses yang masih bersifat reaktif, hanya dilakukan saat ada pengaduan.
6. Nir-Sangkal (*Non-Repudiation*): Audit log terpusat telah tersedia dan dilindungi dari manipulasi. Namun, implementasi tanda tangan digital belum menyeluruh, analisis log masih bersifat reaktif, dan standar pengelolaan log belum seragam antaraplikasi.

5.2 Saran

1. Saran untuk rumah sakit

Berdasarkan hasil penelitian, beberapa rekomendasi yang dapat diberikan kepada Rumah Sakit X adalah sebagai berikut:

a. Rumah sakit perlu melaksanakan audit keamanan informasi secara berkala dan terstruktur, termasuk pengujian kerentanan sistem (*penetration testing*) dan evaluasi efektivitas enkripsi. Selain itu, pelatihan keamanan data bagi seluruh staf perlu dilakukan secara rutin dan berkesinambungan agar budaya keamanan informasi dapat terbentuk sesuai prinsip *continual improvement* dalam ISO/IEC 27001:2022.
b. Rumah sakit disarankan menyediakan pelatihan khusus terkait pengisian rekam medis elektronik yang berfokus pada peningkatan akurasi data dan pemanfaatan fitur sistem secara optimal. Selain itu, diperlukan pengembangan fitur validasi otomatis pada SIMRS untuk membantu mendeteksi potensi kesalahan input sebelum data tersimpan di dalam sistem.
c. Pengadaan server cadangan di lokasi terpisah (*offsite Backup*) perlu segera direalisasikan, baik melalui penyediaan infrastruktur fisik tambahan maupun penggunaan layanan *cloud storage* terenkripsi. Rumah sakit juga perlu menyusun dan menguji disaster *recovery* plan secara berkala agar kesiapan menghadapi kondisi darurat dapat terjamin dan risiko kehilangan data dapat diminimalkan.
d. Rumah sakit disarankan berkoordinasi dengan vendor SIMRS untuk mengintegrasikan *Multi-Factor Authentication* (MFA) pada sistem utama. Selain itu, kebijakan manajemen kata sandi perlu diperkuat melalui pengaturan teknis yang mewajibkan pergantian *password* secara berkala serta penerapan sanksi terhadap praktik berbagi akun antarstaf.
e. Rumah sakit perlu mengembangkan sistem pemantauan akses secara *real-time*, misalnya melalui penerapan Security Information and Event Management (SIEM) atau fitur automated alerting. Dengan demikian, aktivitas mencurigakan dapat segera terdeteksi dan ditangani secara proaktif sebelum berkembang menjadi insiden keamanan yang lebih besar.
f. Implementasi tanda tangan digital perlu diperluas pada seluruh jenis entri rekam medis elektronik agar aspek pembuktian hukum dan perlindungan tenaga kesehatan semakin kuat. Selain itu, rumah sakit disarankan mulai mempersiapkan sertifikasi ISO/IEC 27001 secara bertahap guna memperkuat pengelolaan keamanan informasi sesuai standar internasional.

2. Saran untuk peneliti selanjutnya

Peneliti selanjutnya disarankan untuk melakukan kajian yang lebih mendalam dengan menggunakan metode observasi langsung terhadap sistem SIMRS guna mengidentifikasi kerentanan teknis yang tidak dapat terungkap hanya melalui wawancara. Selain itu, penelitian lanjutan juga dapat memfokuskan pada pengukuran tingkat kematangan (*maturity level*) keamanan informasi sehingga keamanan informasi rumah sakit dapat dipetakan secara lebih terukur

6. REFERENSI

Agreindra, M., Akbar, H. Y. H., & Mahardika, F. (2024). Keamanan Teknologi Informasi: Teori, Risiko, Dan Strategi Pertahanan Di Era Digital.

Ardianto, E. T., Pratiwi, A. N., & Elisanti, A.

D. (2025). Penerapan Hukum Benford Dalam Mendeteksi Potensi Fraud Pada Data Klaim JKN Rawat Inap Di RS X. 4(2), 9–14.

Artiningsih, D. W., Zamrudi, Z., & Herawati, A. S. (2026). Efektivitas Sistem Informasi Dalam Meningkatkan Kualitas Pelayanan Ruang ICU / ICCU (Studi Kasus Pada Ruang ICU / ICCU RSUD Sultan Suriansyah Kota Banjarmasin). 4(3), 17047–17054.

Daniswara, M. C., Putrawanto, D. I., Najib, M., & Achmadha, Z. (2023). Evaluasi Keamanan Informasi Di Lingkungan Rumah Sakit : Pendekatan Audit ISO 27001 Di RS Rahman Rahim Sidoarjo. 3(2), 64–69.

Dewi, N. J., Firdonsyah, A., & Wijayanto, D. (2025). Two Factor Authentication Pada Sistem Login Rekam Medis Elektronik Berbasis Web Menggunakan Metode Prototype. 3, 168–180.

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

Ekasari, D. D. (2025). Tinjauan Keamanan Data Dan Informasi Dalam Penyelenggaraan RME Berdasarkan Permenkes No 24 Tahun 2022 Di RSUD Waras Wiris Boyolali. 1–119.

Ikawati, F. R., Ansyori, A., Anggih, D., & Permatasari, S. (2025). Analisis Keamanan Data Rekam Medis Elektronik Di Fasilitas Kesehatan. 10(2), 230–237.

Jauhary, H., Pratiwi2, G. E., Salim, A. Z., & Fitroh, F. (2022). Penerapan ISO27001 Dalam Menjaga Dan Meminimalisir Risiko Keamanan Informasi : Literatur Review. Media Jurnal Informatika, 14(1), 43. Https://Doi.Org/10.35194/Mji.V14i1.1581

Kominfo, D. (2021). Arsitektur Keamanan SPBE.

Luvi, J. D., Herfin, M., Akbar, M., Saputra, S., Djusmin, V. Bin, Ni'matu, Zuliana, Ardila, N. M. I., Poonwong, P., & Bawias, J. S. C. (2025). Kesiapan Dan Keamanan Infrastruktur Penyelenggaraan Rekam Medis Elektronik Di RSUD Kabupaten Kediri. Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi, 4(2), 157–164. Https://Doi.Org/10.20885/Snati.V4.I2.40288

Melisa, N. P., Sukmaningsih, W. R., & Licia, R. (2024). Analisis Rekam Medis Elektronik Rawat Jalan Pada Aspek Keamanan Data Pasien Di Rumah Sakit Umum Daerah Dr . Soediran Mangun Sumarso Wonogiri. 03(03), 160–168.

Mulyani, W., Kurniasih, D. L. S., & Sukawan, A. (2023). Hak Akses Pelepasan Informasi Rekam Medis Elektronik Untuk Kepentingan Penelitian Di RSUP Dr.Hasan Sadikin Bandung. Jurnal Kebijakan Kesehatan Indonesia, 12(03), 154–159.

Nurandini, N. I., & Ade Irma Suryani. (2024). Tinjauan Aspek Legalitas Dan Keamanan Penggunaan Tanda Tangan Elektronik Pada Rekam Medis Elektronik Di Rumah Sakit X Kota Cimahi. 19(1978), 4015–4022.

Permenkes. (2022). Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis. 1–20.

Permenkes, R. (2020). Peraturan Menteri Kesehatan Republik Indonesia Nomor 3 Tahun 2020 Tentang Klasifikasi Dan Perizinan Rumah Sakit. 3, 1–80.

Prastawa, R. H., Monica, R. D., & Soelistijaningroem, M. (2025). Analisis Penggunaan Fitur Keamanan Dan Privasi Data Dalam Sistem Rekam Medis Elektronik (RME) Di RSUD Al. Journal Of Innovative And Creativity, 5(2), 14549–14556.

Prof. Dr. Sugiyono. (2020). Metode Penelitian Kuantitatif Kualitatif Dan R&D. Alvabeta, CV.

Programme, N. A. P. (2022). ISO 27001:2022 Information Security Implementation Guide. Https://Www.Nqa.Com/Getmedia/Ae12c945-4dbb-4b73-A4e3-996261a540af/NQA-ISO-27001-Implementation-Guide.Pdf

Puteri, D., Pramesti, A., Ayuningtyas, D., & Verdi, R. (2024). Keamanan Dan Kerahasiaan Data Medis Pasien Dalam Implementasi Rekam Medis Elektronik : 8, 7691–7702.

Republik Indonesia. (2022). Undang Undang No.27 Tahun 2022 Tentang Perlindungan Data Pribadi. 016999.

Septiana, A. P., Fatuhu, M. S., Komang, N., Yanti, W., & Khairan, F. (2025). Tinjauan Keamanan Data Rekam Medis Elektronik Pasien Di RSUD Patut Patuh Patju Gerung Lombok Barat. 13(2), 179–185. Https://Doi.Org/10.37824/Jkqh.V13i1.2025

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.

Soraya, O, E. N., & Mawan, M. S. A. (2025). Evaluasi Keamanan Dan Privasi Sistem Rekam Medis Elektronik: Studi Kasus Di Rumah Sakit Wava Husada. 9831(2722), 1–12.

Sulrieni, I. N., Syahputra, M., & Sari, I. (2025). Literature Review : Evaluasi Efektivitas Dan Keamanan Rekam Medis Elektronik Melalui Pendekatan Teknologi Terkini Dalam Layanan Kesehatan. 4(3), 7534–7540.

Syapitri, H., Amila, & Aritonang, J. (2021). Buku Ajar Metodologi Penelitian Kesehatan.

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), 31–38.

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.

Widiyanti, S. W., Hastuti, N. M., & Kusumawati, E. A. (2024). Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi SIMPUS Berdasarkan Aspek Confidentiality, Integrity, Dan Availability Di Puskesmas Tasikmadu Karanganyar. 4(2), 1–6.