Jurnal Manajemen Kesehatan Yayasan RS. Dr. Soetomo Vol.11 No.2 Oktober 2025
Print ISSN 2477-0140 Online ISSN 2581-219X
www.jurnal.stikes-yrsds.ac.id

Evaluasi Manajemen Risiko Terkait Keamanan Data Rekam Medis Elektronik Di Rumah Sakit Mata Undaan Surabaya

Evaluation Of Risk Management Related To Electronic Medical Record Data Security At Undaan Hospital Surabaya

Udin Apriliansyah[1], **Agusta Dian Ellina**[2], **Rahmania Ambarika**[3]
[1,2,3]Universitas STRADA Indonesia
(e-mail: udinapriliansyah@gmail.com, Perum Western Village C5-16 Surabaya)

ABSTRAK

Transformasi digital di sektor kesehatan membawa tantangan baru terhadap keamanan data pasien, khususnya dalam penggunaan sistem Rekam Medis Elektronik (RME). Penelitian ini bertujuan mengevaluasi efektivitas manajemen risiko keamanan data pasien di RS Mata Undaan Surabaya dan memberikan rekomendasi perbaikannya. Metode yang digunakan adalah kualitatif dengan pendekatan fenomenologi, melalui wawancara mendalam terhadap 12 informan dan 3 triangulator, observasi non-partisipatif, serta telaah dokumen. Analisis dilakukan secara tematik dan diperkuat dengan pendekatan *Failure Mode and Effect Analysis* (FMEA) pada 20 subproses. Hasil menunjukkan kelemahan dalam kebijakan formal, hak akses, autentikasi, dan pelaporan insiden. FMEA mengidentifikasi sepuluh subproses dengan nilai RPN tinggi. Rekomendasi mencakup pembentukan kebijakan tertulis, autentikasi berlapis, pembatasan akses berbasis peran, pelatihan rutin, dan uji restore backup. Penelitian ini menekankan pentingnya pendekatan terintegrasi dalam membangun sistem keamanan RME yang tangguh dan berkelanjutan

Kata kunci : Keamanan data, rekam medis elektronik, manajemen risiko, FMEA, rumah sakit

ABSTRACT

Digital transformation in the healthcare sector brings new challenges to patient data security, particularly in the use of the Electronic Medical Record (EMR) system. This study aims to evaluate the effectiveness of patient data security risk management at Undaan Eye Hospital Surabaya and provide recommendations for improvement. The method used was qualitative with a phenomenological approach, through in-depth interviews with 12 informants and 3 triangulators, non-participatory observation, and document review. The analysis was done thematically and strengthened with the Failure Mode and Effect Analysis (FMEA) approach on 20 subprocesses. Results showed weaknesses in formal policies, access rights, authentication, and incident reporting. FMEA identified ten subprocesses with high RPN values. Recommendations include the establishment of written policies, layered authentication, role-based access restrictions, regular training, and test restore backups. This research emphasizes the importance of an integrated approach in building a resilient and sustainable EMR security system.

Keywords: Data security, electronic medical record, risk management, FMEA, hospital

PENDAHULUAN

Transformasi digital dalam sektor pelayanan kesehatan telah membawa perubahan signifikan dalam manajemen informasi pasien, salah satunya dengan adopsi sistem Rekam Medis Elektronik (RME). RME memungkinkan penyimpanan, pengelolaan, dan pertukaran data medis pasien secara efisien dan *real-time* di berbagai unit pelayanan kesehatan (Cita et al., 2025). Namun, seiring dengan meningkatnya ketergantungan terhadap sistem digital, muncul pula tantangan baru terkait perlindungan data, khususnya menyangkut aspek keamanan, kerahasiaan, dan integritas data pasien. Isu ini menjadi semakin penting karena data medis tergolong sebagai data pribadi yang sangat sensitif dan wajib dilindungi. Dalam konteks hukum di Indonesia, perlindungan terhadap data pribadi, termasuk data kesehatan, telah diatur secara spesifik dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang menegaskan bahwa pengendali data wajib menjamin keamanan informasi dari risiko kebocoran, kehilangan, atau penyalahgunaan oleh pihak tidak berwenang.

Dalam praktiknya, berbagai risiko yang melekat pada sistem RME seperti kebocoran data, serangan malware, penyalahgunaan hak akses, hingga kegagalan sistem (*system failure*) dapat menimbulkan dampak serius tidak hanya bagi individu pasien, tetapi juga terhadap reputasi rumah sakit dan kepercayaan publik terhadap layanan kesehatan digital (Hatton et al., 2012). Beberapa studi internasional menunjukkan bahwa sistem informasi kesehatan di negara berkembang sering kali belum dibarengi dengan kesiapan manajerial dan teknis yang memadai. Penelitian Ayatollahi, mengungkap bahwa rumah sakit di negara berkembang cenderung menerapkan kebijakan keamanan informasi yang reaktif, tanpa sistem evaluasi berkelanjutan atau strategi mitigasi risiko yang terdokumentasi dengan baik (Ayatollahi & Shagerdi, 2017). Studi tersebut juga menekankan pentingnya sinergi antara teknologi, prosedur, dan sumber daya manusia sebagai elemen utama keberhasilan sistem keamanan informasi.

Di Indonesia, tantangan serupa juga muncul. Penelitian Pujihastuti (2021) menyatakan bahwa tingkat kesadaran staf terhadap keamanan digital masih rendah, dan diseminasi kebijakan keamanan belum berjalan optimal (Pujihastuti, 2021). Hal ini menyebabkan lemahnya kepatuhan terhadap prosedur standar yang berujung pada peningkatan potensi insiden pelanggaran data. Observasi awal peneliti di Rumah Sakit Mata Undaan Surabaya mengindikasikan adanya celah-celah serius dalam pengelolaan risiko keamanan data. Tiga insiden yang cukup mencolok yaitu downtime sistem pada tahun 2018, kejadian gagal simpan data pada tahun 2023, serta kebakaran ruang server pada awal 2024 menunjukkan belum matangnya sistem mitigasi risiko dan kesiapan

infrastruktur rumah sakit dalam menghadapi gangguan teknis. Dampak dari insiden tersebut tidak hanya bersifat teknis, namun juga memengaruhi kesinambungan pelayanan dan ketepatan informasi dalam pengambilan keputusan klinis (Tamin & Hendrik, 2025).

Menyikapi hal tersebut, berbagai kerangka kerja keamanan data seperti ISO/IEC 27001 telah banyak digunakan sebagai acuan standar internasional dalam menyusun kebijakan dan prosedur keamanan informasi. Di samping itu, pendekatan *Failure Mode and Effect Analysis* (FMEA) yang umum diterapkan dalam manajemen risiko klinis juga mulai banyak diadaptasi untuk mengevaluasi potensi kegagalan pada sistem informasi digital, termasuk sistem RME (Carlson, 2012). FMEA memungkinkan identifikasi titik-titik lemah dalam alur proses, penilaian tingkat risiko berdasarkan *severity, occurrence,* dan *detectability,* serta penyusunan prioritas mitigasi yang sistematis. Sayangnya, integrasi pendekatan manajemen risiko seperti FMEA dalam konteks keamanan data RME di Indonesia masih belum banyak ditemukan, khususnya yang berbasis pada pengalaman pengguna sistem dan wawancara mendalam lintas fungsi (We'e et al., 2023).

Penelitian ini memiliki nilai kebaruan karena tidak hanya menilai aspek teknis dari sistem keamanan data RME, melainkan juga menelaah dimensi kebijakan, operasional, budaya kerja, dan kesiapan sumber daya manusia di lingkungan rumah sakit (Ikawati, 2024). Dengan menggunakan pendekatan kualitatif fenomenologis, penelitian ini menggali pengalaman nyata pengguna sistem RME, triangulasi dari manajer TI, vendor, dan tim percepatan RME, serta memperkuat analisis dengan pendekatan evaluasi risiko menggunakan FMEA terhadap 20 subproses utama. Pendekatan ini diharapkan mampu memberikan gambaran menyeluruh tentang efektivitas manajemen risiko yang telah diterapkan, serta mengidentifikasi celah-celah sistemik yang perlu segera diperbaiki (Melisa et al., 2024).

Tujuan dari penelitian ini adalah untuk mengevaluasi efektivitas penerapan manajemen risiko keamanan data pasien dalam sistem RME di Rumah Sakit Mata Undaan Surabaya. Fokus evaluasi mencakup lima aspek utama, yaitu sejauh mana sistem manajemen risiko diterapkan, kelemahan yang masih ada, efektivitas pengendalian yang sudah dilakukan, langkah mitigasi terhadap potensi insiden, serta menyusun rekomendasi perbaikan yang praktis dan aplikatif untuk meningkatkan ketahanan sistem keamanan data pasien di era digital.

METODE

Penelitian ini menggunakan metode kualitatif dengan desain fenomenologi, yang bertujuan untuk mengeksplorasi pengalaman, pemahaman, dan praktik para pengguna serta pengelola sistem Rekam Medis Elektronik (RME) dalam konteks keamanan data pasien di Rumah Sakit Mata Undaan Surabaya (We'e et al., 2023). Penelitian dilaksanakan di RS Mata Undaan Surabaya pada periode Januari hingga April 2025. Informan terdiri dari 12 responden utama yang merupakan pengguna sistem RME dari berbagai unit, serta 3 triangulator kunci, yakni manajer TI, vendor RME, dan ketua tim percepatan RME. Pemilihan informan dilakukan dengan teknik purposive sampling berdasarkan keterlibatan langsung dalam pengelolaan dan penggunaan sistem.

Teknik pengumpulan data dilakukan melalui wawancara mendalam dengan panduan semi-terstruktur, observasi non-partisipatif terhadap aktivitas penggunaan sistem, serta studi dokumentasi kebijakan dan insiden keamanan data. Analisis data dilakukan secara tematik dengan pendekatan induktif, yang mencakup proses transkripsi, pengkodean, kategorisasi, dan identifikasi tema utama yang muncul (Budiman et al., 2025). Untuk memperkuat validitas, dilakukan triangulasi sumber, metode, dan waktu, serta pemeriksaan keabsahan data melalui member check dan diskusi antar peneliti. Evaluasi risiko juga dilengkapi dengan pendekatan *Failure Mode and Effect Analysis* (FMEA) terhadap 20 subproses sistem RME, yang digunakan untuk mengidentifikasi titik rawan dan memprioritaskan mitigasi berdasarkan nilai *Risk Priority Number* (RPN). Penyajian data dilakukan secara naratif dan didukung tabel serta matriks risiko untuk memperjelas temuan lapangan secara sistematis (Jones et al., 2012). Penelitian ini telah mendapat Surat Keterangan kelaiakan Etik/ *Ethical Clearance* dari Komite Etik Penelitian Kesehatan Universitas STRADA Indonesia dengan Nomor: 0523443/EC/KEPK/I/04/2025.

HASIL

Subjek dalam penelitian ini terdiri dari 12 informan utama yang merupakan pengguna sistem Rekam Medis Elektronik (RME) di Rumah Sakit Mata Undaan Surabaya, dengan latar belakang profesi yang beragam, mulai dari tenaga medis, petugas administrasi, hingga staf manajemen rekam medis. Selain itu, triangulasi data dilakukan dengan melibatkan tiga informan kunci yaitu Manajer Teknologi Informasi, vendor penyedia sistem RME, serta Ketua Tim Percepatan RME (Sittig & Singh, 2010). Para

informan dipilih berdasarkan keterlibatan aktif mereka dalam implementasi dan pengelolaan sistem keamanan data RME.

Hasil penelitian menunjukkan bahwa penerapan manajemen risiko di RS Mata Undaan belum sepenuhnya sistematis. Praktik pengendalian lebih banyak bersifat teknis dan adaptif, seperti pembatasan hak akses, penggunaan akun individu, dan backup data rutin. Namun, belum terdapat kebijakan institusional formal dan terdokumentasi yang mengatur secara menyeluruh langkah-langkah manajemen risiko informasi. Pengetahuan staf masih terbatas pada prinsip dasar keamanan digital, sementara implementasi prosedur seperti *logout* dan pengawasan akun belum berjalan optimal (Asih et al., 2024).

Penelitian mengidentifikasi empat kelemahan utama dalam sistem keamanan data: (1) tidak meratanya diseminasi kebijakan keamanan informasi; (2) praktik penggunaan akun bersama dan lemahnya budaya pelaporan insiden; (3) keterbatasan infrastruktur teknologi seperti kapasitas server dan kecepatan akses saat beban tinggi; dan (4) belum adanya mekanisme monitoring risiko secara berkala. Hal ini menunjukkan sistem belum mengadopsi pendekatan closed-loop dalam siklus manajemen risiko (Budiman et al., 2025).

Pengendalian risiko telah dilakukan melalui tiga pendekatan: teknis (*role-based access control, firewall*, antivirus), operasional (pencatatan manual saat *downtime*), dan preventif (*backup* dua kali sehari). Namun efektivitasnya masih terbatas karena minimnya audit teknis dan tidak adanya indikator evaluatif. Pengendalian yang dilakukan belum terintegrasi dalam sistem mutu atau strategi jangka panjang. Peneliti menilai, strategi pengendalian saat ini lebih bersifat reaktif ketimbang proaktif (Neng Sari Rubiyanti, 2023).

Berdasarkan analisis *Failure Mode and Effect Analysis* (FMEA) terhadap 20 subproses yang terkait dengan keamanan data dalam sistem Rekam Medis Elektronik (RME), penelitian ini menemukan bahwa terdapat tiga subproses dengan nilai *Risk Priority Number* (RPN) tertinggi yang memerlukan perhatian khusus dalam strategi mitigasi risiko. Ketiga subproses tersebut adalah: (1) pengaturan hak akses yang terlalu luas, (2) belum diterapkannya autentikasi ganda (*multi-factor authentication* atau MFA), dan (3) potensi kesalahan input data pasien. Ketiga aspek ini dinilai memiliki dampak signifikan terhadap integritas, kerahasiaan, dan ketersediaan data pasien apabila tidak ditangani dengan baik (Carlson, 2012). Hak akses yang terlalu luas berisiko membuka

celah bagi penyalahgunaan informasi, terutama jika pengguna sistem dapat mengakses data di luar tanggung jawab atau wewenangnya. Tanpa adanya pembatasan berbasis peran yang ketat (*role-based access control*), potensi pelanggaran privasi dan kebocoran data menjadi lebih tinggi (Endah Wardani et al., 2024). Berikut hasil perhitungan nilai RPN dari analisis FMEA disajikan pada Tabel 1, untuk menunjukkan subproses dengan tingkat prioritas risiko tertinggi yang dapat menjadi dasar pengambilan keputusan dalam strategi mitigasi ke depan.

Tabel 1. Subproses dengan Nilai RPN Tertinggi berdasarkan Analisis FMEA

Modus Kegagalan Potensial	Efek Potensial dari Kegagalan	Penyebab Potensial dari kegagalan	Pengendalian yang sudah ada Saat Ini	S	O	D	RPN
Penentuan hak akses sesuai peran (*role-based access*)	Pengguna mengakses data yang bukan wewenangnya; potensi pelanggaran privasi	Tidak dilakukan konfigurasi *role-based access* secara spesifik	SPO Keamanan Data Dan Informasi, Juknis Rekam Medis Elektronik	5	4	5	100
Penggunaan sistem autentifikasi (password / MFA)	Risiko pembobolan akun meningkat jika password diketahui orang lain	Sistem hanya menggunakan password standar	SPO Keamanan Data Dan Informasi	5	3	5	75
Input data pasien oleh tenaga medis/admin	Kesalahan rekam medis; dampak pada diagnosis atau tindakan medis	Kurang pelatihan; tidak ada validasi setelah input	Juknis Rekam Medis Elektronik	4	4	4	64
Akses dan pembacaan data oleh pengguna lain	Pengguna lain bisa akses data pasien tanpa otorisasi	*Login* masih aktif; komputer tidak di*logout*	SPO Keamanan Data Dan Informasi, Juknis RME	5	3	4	60
Pengamanan fisik ruang server (akses terbatas, proteksi kebakaran)	Potensi sabotase, pencurian perangkat, dan modifikasi sistem	Ruang server tidak dikunci atau tidak dijaga	SPO Pemeliharaan Server, SPO Keamanan Ruang Server (Akses)	4	3	5	60
Deteksi akses mencurigakan dan pelaporan otomatis	Kejadian *login* ilegal tidak segera diketahui atau dicegah	Tidak ada fitur sistem untuk mendeteksi akses abnormal	SPO Keamanan Data Dan Informasi	4	3	5	60
Monitoring log aktivitas pengguna	Aktivitas mencurigakan tidak diketahui, insiden bisa	Tidak ada penanggung jawab khusus, sistem	SPO Keamanan Data Dan	3	4	5	60

Modus Kegagalan Potensial	Efek Potensial dari Kegagalan	Penyebab Potensial dari kegagalan	Pengendalian yang sudah ada Saat Ini	S	O	D	RPN
	terulang	monitoring pasif					
Monitoring log aktivitas pengguna	Aktivitas mencurigakan tidak diketahui, insiden bisa terulang	Tidak ada penanggung jawab khusus, sistem monitoring pasif	SPO Keamanan Data Dan	3	4	5	60
Backup data secara berkala oleh tim TI	Kehilangan data jika terjadi kerusakan sistem	Jadwal tidak dicek rutin, proses otomatis gagal tanpa disadari	SPO Downtime system tidak terjadwal, SPO downtime Sistem Terjadwal	5	2	5	50
Pembuatan akun dan otorisasi pengguna baru	Orang tidak berhak bisa memperoleh akses ke sistem RME	Tidak ada verifikasi otorisasi pengguna dari Manajer	SPO Keamanan Data Dan Informasi, Juknis Rekam Medis Elektronik	4	3	4	48
Pengujian pemulihan data (*restore test*)	Saat dibutuhkan, file backup tidak dapat digunakan dengan cepat	Belum ada simulasi pemulihan data rutin	SOP *Restore Data Base*	4	3	4	48

Keterangan: S = *Severity*/ Dampak; O = *Occurance*/ Probabilitas; D = *Detection*/ Deteksi

Meskipun rumah sakit telah melakukan beberapa upaya mitigasi seperti backup data secara otomatis, penggunaan SOP keamanan, dan pelatihan awal kepada staf baru, namun langkah-langkah tersebut belum sepenuhnya menjangkau permasalahan yang bersifat sistemik dan teknis. Beberapa kebijakan belum diformalkan secara menyeluruh, dan pelatihan berkala atau simulasi insiden belum dijalankan secara sistematis (Simanjuntak et al., 2025). Oleh karena itu, ketiga subproses ini menjadi prioritas untuk intervensi, baik melalui penguatan kebijakan internal, peningkatan teknologi keamanan, maupun peningkatan kompetensi dan kesadaran staf terhadap pentingnya perlindungan data pasien. Penguatan pada aspek-aspek ini akan secara langsung berkontribusi terhadap peningkatan ketahanan sistem RME dan perlindungan informasi kesehatan yang lebih baik.

Rekomendasi difokuskan pada lima aspek utama: (1) penyusunan kebijakan formal dan SOP berbasis risiko; (2) peningkatan kapasitas infrastruktur dan penggunaan cloud terenkripsi; (3) pelatihan rutin berbasis studi kasus nyata; (4) integrasi hak akses dengan sistem kepegawaian secara otomatis; dan (5) pembentukan tim keamanan

informasi lintas unit. Pendekatan ini bertujuan memperkuat resiliensi organisasi dan memastikan bahwa keamanan data menjadi bagian dari budaya kerja, bukan sekadar tanggung jawab teknis.

PEMBAHASAN

Permasalahan keamanan data dalam sistem Rekam Medis Elektronik (RME) tidak hanya berkutat pada kekuatan teknologi informasi yang digunakan, tetapi juga mencerminkan sejauh mana kesiapan institusi dalam menerapkan prinsip manajemen risiko secara komprehensif (Tasbihah & Yunengsih, 2024). Berdasarkan penerapan metode *Failure Mode and Effect Analysis* (FMEA), penelitian ini mengidentifikasi tiga subproses dengan nilai *Risk Priority Number* (RPN) tertinggi yang menuntut perhatian segera, yakni pengaturan hak akses pengguna, belum digunakannya autentikasi ganda (*multi-factor authentication*), serta kesalahan input data pasien (Carlson, 2012).

Permasalahan hak akses yang terlalu luas menunjukkan bahwa prinsip *least privilege* belum sepenuhnya dijalankan. Idealnya, setiap pengguna hanya memiliki akses terbatas sesuai perannya dalam sistem. Namun, temuan di lapangan memperlihatkan bahwa beberapa pengguna masih dapat mengakses data yang tidak termasuk dalam lingkup tanggung jawabnya. Hal ini menimbulkan risiko terhadap pelanggaran privasi dan kebocoran data pasien, dan mencerminkan lemahnya pengendalian administratif. Panduan ISO/IEC 27001 secara eksplisit menyebutkan bahwa pengendalian akses berbasis peran (*role-based access control*) merupakan elemen fundamental dalam membangun sistem keamanan informasi yang andal. Temuan ini juga sejalan dengan penelitian Mukharram, yang menyimpulkan bahwa lemahnya pembatasan akses merupakan faktor pemicu utama terjadinya insiden pelanggaran data pribadi di sektor kesehatan (Mukharram et al., 2024).

Risiko kedua berkaitan dengan belum digunakannya autentikasi ganda dalam proses login pengguna. Saat ini, sistem RME di RS Mata Undaan hanya menggunakan autentikasi satu faktor, yaitu kombinasi nama pengguna dan kata sandi. Padahal, pendekatan autentikasi ganda atau *multi-factor authentication* (MFA) telah diakui sebagai salah satu strategi pertahanan paling efektif dalam menghadapi serangan siber, terutama untuk melindungi data sensitif seperti rekam medis. Ayatollahi et al. (2019) menegaskan bahwa MFA dapat secara signifikan mengurangi risiko akses tidak sah karena mempersempit peluang penyalahgunaan kredensial yang bocor (Ayatollahi & Shagerdi, 2017). Ketidakhadiran MFA menunjukkan belum optimalnya pendekatan *defense in*

depth dalam desain sistem informasi yang diterapkan.

Risiko ketiga adalah masih terjadinya kesalahan input data oleh tenaga medis atau admin. Kesalahan ini umumnya bersumber dari tidak adanya mekanisme verifikasi data setelah entri dilakukan, kurangnya pelatihan berkala, serta tekanan beban kerja. Temuan ini sejalan dengan hasil penelitian Kim yang menyebutkan bahwa kesalahan input sering kali disebabkan oleh faktor non-teknis seperti kelelahan staf, keterbatasan pelatihan, dan minimnya protokol validasi (Kim et al., 2017). Dalam jangka panjang, kesalahan entri data dapat mengganggu pengambilan keputusan medis dan menurunkan kualitas pelayanan.

Selain ketiga risiko tersebut, hasil penelitian juga menunjukkan belum adanya sistem deteksi dini (*early warning system*) seperti pemantauan log aktivitas secara real-time atau sistem alert otomatis terhadap aktivitas mencurigakan. Sistem saat ini lebih bersifat reaktif, di mana insiden baru ditangani setelah terjadi, bukan dicegah sejak dini. Kondisi ini menandakan bahwa prinsip deteksi dan respons cepat sebagaimana dianjurkan dalam ISO/IEC 27035 belum sepenuhnya diimplementasikan secara menyeluruh.

Aspek lain yang tidak kalah penting adalah belum dilakukannya uji pemulihan data (*restore test*) secara terjadwal. Walaupun proses backup telah berjalan secara otomatis dua kali sehari, ketidakpastian terhadap validitas file cadangan akan terus menjadi potensi risiko, terutama ketika terjadi insiden besar seperti kerusakan server. Sittig dan Singh (2016) menyatakan bahwa organisasi yang tidak secara aktif menguji sistem cadangannya cenderung mengalami hambatan besar dalam proses pemulihan saat bencana digital terjadi. Dengan kata lain, *disaster recovery plan* yang tidak teruji justru berpotensi menambah beban saat insiden berlangsung (Darmiani et al., 2024).

Dari sintesis berbagai temuan dan referensi di atas, terlihat bahwa manajemen risiko keamanan data di RS Mata Undaan Surabaya masih bersifat parsial dan belum dibingkai dalam pendekatan holistik yang menggabungkan kebijakan, teknologi, prosedur, serta kesadaran individu. Penelitian Pujihastuti (2021) menegaskan pentingnya kolaborasi antara struktur kebijakan dan pemahaman pengguna sebagai pilar keberhasilan sistem keamanan data rumah sakit (Pujihastuti, 2021). Dalam konteks ini, pendekatan adaptif dan pembelajaran berkelanjutan dari setiap insiden menjadi sangat penting dalam membangun ketahanan sistem jangka panjang.

Penelitian ini tidak hanya berfokus pada aspek teknis, tetapi juga mengintegrasikan analisis mendalam terhadap dimensi kebijakan, operasional, sumber daya manusia, dan budaya kerja melalui pendekatan kualitatif fenomenologis yang

melibatkan pengguna langsung, manajer TI, vendor, dan tim percepatan RME. Selain itu, penelitian ini mengadaptasi metode Failure Mode and Effect Analysis (FMEA), yang umumnya digunakan dalam konteks klinis, untuk mengidentifikasi dan memprioritaskan risiko pada sistem informasi digital, khususnya RME, dengan menganalisis 20 subproses utama (Carlson, 2012). Hal ini menghasilkan identifikasi titik kritis yang spesifik dan rekomendasi mitigasi yang aplikatif, seperti perlunya autentikasi ganda, pembatasan hak akses berbasis peran, serta uji pemulihan data yang terjadwal, yang belum banyak diterapkan atau terdokumentasi dalam studi serupa di Indonesia. Dengan demikian, penelitian ini tidak hanya mengisi celah literatur tetapi juga menawarkan kerangka evaluasi yang holistik dan relevan bagi pengembangan tata kelola keamanan data RME di institusi kesehatan lokal.

Meskipun penelitian ini bersifat kualitatif dan belum dilengkapi audit teknis seperti *penetration testing*, kontribusinya tetap signifikan, terutama dalam mengidentifikasi area kritis yang memerlukan perbaikan. Penelitian lanjutan disarankan untuk mengadopsi pendekatan kuantitatif atau simulasi teknis guna mengukur efektivitas kontrol secara lebih objektif dan terstandarisasi. Refleksi terhadap hasil ini menunjukkan bahwa rumah sakit tidak hanya perlu berinvestasi dalam teknologi, tetapi juga dalam edukasi pengguna, pengembangan kebijakan, dan perencanaan kontinjensi yang teruji secara sistematik. Penelitian ini diharapkan dapat menjadi landasan awal bagi pembentukan kebijakan keamanan informasi yang lebih kuat, kontekstual, dan sesuai dengan dinamika layanan kesehatan digital di Indonesia.

Studi ini memiliki beberapa keterbatasan, ruang lingkup metodologi yang bersifat kualitatif sehingga temuan tidak dapat digeneralisasi secara luas, ketiadaan audit teknis mendalam seperti *penetration testing* atau simulasi serangan siber yang dapat mengonfirmasi kerentanan secara empiris, serta fokus pada satu rumah sakit sehingga temuan mungkin tidak mewakili kondisi seluruh institusi kesehatan dengan karakteristik berbeda. Selain itu, data yang dikumpulkan sangat bergantung pada wawancara dan persepsi subjek penelitian, yang berpotensi mengandung bias subjektivitas, serta tidak mencakup evaluasi menyeluruh terhadap semua aspek teknis seperti konfigurasi jaringan, enkripsi data, atau keamanan fisik secara detail. Meskipun menggunakan FMEA untuk analisis risiko, penghitungan Risk Priority Number (RPN) juga bergantung pada penilaian peneliti yang dapat dipengaruhi oleh interpretasi dan pengalaman subjek.

SIMPULAN

Berdasarkan hasil penelitian dengan pendekatan kualitatif dan metode FMEA, disimpulkan bahwa pengelolaan risiko keamanan data pada sistem Rekam Medis Elektronik (RME) di Rumah Sakit Mata Undaan Surabaya masih memerlukan penguatan signifikan, terutama karena adanya kesenjangan dalam tiga pilar utama: kebijakan, prosedur, dan teknologi. Identifikasi risiko mengungkap sepuluh titik kritis, dengan tiga risiko utama berupa hak akses yang terlalu luas, tidak digunakannya autentikasi ganda, dan kesalahan input data, yang disebabkan oleh lemahnya deteksi dini dan tidak adanya prosedur insiden yang baku. Meskipun beberapa kontrol teknis seperti *firewall* dan antivirus telah diterapkan, pengendalian non-teknis seperti pelatihan berkelanjutan dan simulasi penanganan insiden masih kurang. Sebagai tindak lanjut, diperlukan pembentukan tim manajemen risiko digital, pengembangan sistem pelaporan insiden real-time, penerapan autentikasi ganda, log audit aktif, serta *restore testing* yang terjadwal untuk memperkuat ketahanan sistem secara strategis dan berkelanjutan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Direksi dan Manajemen serta karyawan Rumah Sakit Mata Undaan telah mengizinkan kami untuk mendapat data penelitian, serta saran dan bimbingan dari dosen pembimbing dalam proses penelitian.

DAFTAR PUSTAKA

Asih, H. A., Indrayadi, I., Soraya, S., & Khairunnisa, K. (2024). Evaluasi Keamanan Data Pasien Pada Rekam Medis Elektronik Dengan Systematic Literature Review. *Jurnal Ilmiah FIFO*, *16*(2), 104. https://doi.org/10.22441/fifo.2024.v16i2.001

Ayatollahi, H., & Shagerdi, G. (2017). Information Security Risk Assessment in Hospitals. *The Open Medical Informatics Journal*, *11*, 37–43. https://doi.org/10.2174/1874431101711010037

Budiman, A., Isa, M., & Soekiswati, S. (2025). Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RS P Surakarta. *Ranah Research : Journal of Multidisciplinary Research and Development*, *7*(3), 2118–2127. https://doi.org/10.38035/rrj.v7i3.1421

Carlson, C. (2012). Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Mode and Effects Analysis. *Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Mode and Effects Analysis*. https://doi.org/10.1002/9781118312575

Cita, Y., Miranda, A., Fandani, M., Mahputra, S., Aura, I., Irawan, F., & Paramarta, V. (2025). Tantangan Implementasi Simrs Dari Perspektif Tenaga Kesehatan: Studi Kualitatif Di Rumah Sakit Daerah Challenges of Simrs Implementation From the Perspective of Health Personnel: a Qualitative Study in a Regional Hospital. *Multidisciplinary Journal of Counseling and Social Research*, *4*(1), 2962–8350. https://doi.org/10.59027/al-ihtiram.v4i1.965

Darmiani, S., Yuda Pratama, B., Maulani, J., Islamy, B., Arie Hidayat, T., & Paramarta, V. (2024). Tantangan Integrasi Rekam Medis Elektronik dengan Sistem Manajemen Rumah Sakit: Dampak pada Keamanan Data dan Efisiensi Biaya Operasional-A Systematic Review. *Jurnal Sosial Dan Sains*, *4*(11), 1107–1116. https://doi.org/10.59188/jurnalsosains.v4i11.27924

Endah Wardani, Happy Putra, D., Sonia, D., & Yulia, N. (2024). Keamanan Sistem Informasi Rekam Medis Elektronik Di Rumah Sakit Islam Jakarta Sukapura. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, *3*(2 SE-Articles), 31–38. https://doi.org/10.47134/rmik.v3i2.1756

Hatton, J. D., Schmidt, T. M., & Jelen, J. (2012). Adoption of Electronic Health Care Records: Physician Heuristics and Hesitancy. *Procedia Technology*, *5*, 706–715. https://doi.org/10.1016/j.protcy.2012.09.078

Ikawati, F. R. (2024). Efektivitas Penggunaan Rekam Medis Elektronik Terhadap Peningkatan Kualitas Pelayanan Pasien di Rumah Sakit. *Ranah Research : Journal of Multidisciplinary Research and Development*, *6*(3), 282–292. https://doi.org/10.38035/rrj.v6i3.819

Jones, S. S., Heaton, P. S., Rudin, R. S., & Schneider, E. C. (2012). Unraveling the IT productivity paradox--lessons for health care. *The New England Journal of Medicine*, *366*(24), 2243–2245. https://doi.org/10.1056/NEJMp1204980

Kim, M. O., Coiera, E., & Magrabi, F. (2017). Problems with health information technology and their effects on care delivery and patient outcomes: a systematic review. *Journal of the American Medical Informatics Association : JAMIA*, *24*(2), 246–250. https://doi.org/10.1093/jamia/ocw154

Melisa, N., Sukmaningsih, W., & Licia, R. (2024). Analisis Rekam Medis Elektronik Rawat Jalan Pada Aspek Keamanan Data Pasien Di Rumah Sakit Umum Daerah Dr. Soediran Mangun Sumarso Wonogiri. *Journal Health Information Management Indonesian (JHIMI)*, *3*, 160–168. https://doi.org/10.46808/jhimi.v3i3.193

Mukharram, M. F., Nurita, D. P., & Paramarta, V. (2024). Penerapan Rekam Medis Elektronik Di Rumah Sakit. *Journal of Social and Economics Research*, *6*(1 SE-Articles). https://doi.org/10.54783/jser.v6i1.471

Neng Sari Rubiyanti. (2023). Penerapan Rekam Medis Elektronik di Rumah Sakit di Indonesia: Kajian Yuridis. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, *1*(1 SE-Articles), 179–187. https://doi.org/10.59246/aladalah.v1i1.163

Pujihastuti, A. (2021). Penerapan Sistem Informasi Manajemen Dalam

Mendukung Pengambilan Keputusan Manajemen Rumah Sakit. *Jurnal Manajemen Informasi Kesehatan Indonesia*, *9*(2), 200. https://doi.org/10.33560/jmiki.v9i2.377

Simanjuntak, E., Hasibuan, A. S., Lubis, S. P. S., Karo Karo, S., Ritonga, Z., & Hulu, D. (2025). Analisis Penerapan Manajemen Resiko Pada Rekam Medis Elektronik Di Upt Puskesmas Kota Matsum. *Jurnal Ilmiah Pengabdian Kepada Masyarakat (Ji-SOMBA)*, *4*(2 SE-Articles), 88–95. https://doi.org/10.52943/jisomba.v4i2.1901

Sittig, D. F., & Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Quality & Safety in Health Care*, *19 Suppl 3*(Suppl 3), i68-74. https://doi.org/10.1136/qshc.2010.042085

Tamin, Z., & Hendrik, B. (2025). Penerapan Algoritme Advanced Encryption Standard (AES-128) untuk Mengamankan File Rekam Medis Pasien. *Jurnal KomtekInfo*, *12*(1 SE-Articles), 22–30. https://doi.org/10.35134/komtekinfo.v12i1.592

Tasbihah, F., & Yunengsih, Y. (2024). Penerapan Rekam Medis Elektronik dalam Menunjang Efektivitas Kerja Perekam Medis di Rumah Sakit Hasna Medika Cirebon. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *5*(3), 2761–2767. https://doi.org/10.35870/jimik.v5i3.946

We'e, A., Nugroho, H., & Siswatibudi, H. (2023). Evaluasi Aspek Keamanan Dan Kerahasiaan Rekam Medis Elektronik Di Rumah Sakit Panti Nugroho. *Jurnal Permata Indonesia*, *14*(2), 72–81. https://doi.org/10.59737/jpi.v14i2.265

Submission	5 Agustus 2025
Review	12 September 2025
Accepted	14 Oktober 2025
Publish	20 November 2025
DOI	10.29241/jmk.v11i2.2346
Sinta Level	3 (Tiga)
JMK Yayasan RS Dr. Soetomo	Jurnal Manajemen Kesehatan Yayasan RS.Dr.Soetomo p-ISSN 2477-0140, e-ISSN 2581-219X, Volume 11 No.2 2025, DOI: 10.29241/jmk.v11i2.2346 Published by STIKES Yayasan RS.Dr.Soetomo.
	Copyright (c) 2025 Udin Apriliansyah This is an Open Access (OA)article under the CC BY 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).