

Analisis Manajemen Risiko Pada Rekam Medis Elektronik Rawat Jalan Studi Di Rumah Sakit Menggunakan Metode *Failure Mode And Effect Analysis* (FMEA)

Bq Dwi Agustina Rahmawati¹⁾, Resta Dwi Yuliani*²⁾

¹⁾Program Studi Ilmu Kesehatan, Universitas Muhammadiyah Sidoarjo, Indonesia

²⁾ Program Studi Manajemen Informasi Kesehatan, Universitas Muhammadiyah Sidoarjo, Indonesia

*Email Penulis Korespondensi, restadwiyluliani@umsida.ac.id

Abstract. *Electronic Medical Records (EMR) are mandatory in healthcare facilities, yet a preliminary study at RSU 'Aisyiyah Siti Fatimah Tulangan found data duplication and inconsistent EMR entries due to limited system validation. This study analyzes risk management in outpatient EMR using the Failure Mode and Effect Analysis (FMEA) method. This quantitative case study involved 75 outpatient staff (total sampling); data were collected through interviews, observation, and questionnaires, then assessed using Severity, Occurrence, and Detection to calculate RPN ($S \times O \times D$). Results showed four top-priority risks: duplicate data (RPN 192), inconsistent data (RPN 180), absence of automatic log-out (RPN 168), and human error (RPN 120). Mitigation recommendations, based on ISO/IEC 27001:2022, include mandatory data validation, automatic warnings, automatic log-out, staff training, and a ban on account sharing. FMEA proved effective in identifying and prioritizing outpatient EMR risks.*

Keywords - *Electronic Medical Record, Risk Management, FMEA, RPN, ISO/IEC 27001:2022*

Abstrak. *Rekam Medis Elektronik (RME) wajib diterapkan di seluruh fasilitas kesehatan, namun studi pendahuluan di RSU 'Aisyiyah Siti Fatimah Tulangan menemukan duplikasi data dan ketidakkonsistenan pengisian RME akibat keterbatasan fitur validasi sistem. Penelitian ini bertujuan menganalisis manajemen risiko pada RME rawat jalan menggunakan metode Failure Mode and Effect Analysis (FMEA). Penelitian kuantitatif dengan desain studi kasus ini melibatkan 75 petugas rawat jalan (total sampling), data dikumpulkan melalui wawancara, observasi, dan kuesioner, lalu dinilai berdasarkan Severity, Occurrence, dan Detection untuk menghitung RPN ($S \times O \times D$). Hasil menunjukkan empat risiko prioritas tertinggi: duplikasi data (RPN 192), data tidak konsisten (RPN 180), ketiadaan fitur log out otomatis (RPN 168), dan human error (RPN 120). Rekomendasi mitigasi mengacu pada ISO/IEC 27001:2022, meliputi validasi data wajib, peringatan otomatis, log out otomatis, pelatihan petugas, dan larangan berbagi akun. FMEA terbukti efektif mengidentifikasi dan memprioritaskan risiko RME rawat jalan.*

Kata Kunci - *Rekam Medis Elektronik, Manajemen Risiko, FMEA, RPN, ISO/IEC 27001:2022*

I. PENDAHULUAN

Bentuk pengembangan teknologi informasi di layanan kesehatan saat ini adalah migrasi dari sistem konvensional menuju rekam medis elektronik [1]. Rekam medis elektronik merupakan versi digital dari riwayat kesehatan pasien yang mencakup data diri, hasil pengecekan dokter, rencana pengobatan, serta berbagai tindakan medis yang telah dilakukan [2]. Sesuai regulasi yang ditetapkan, seluruh fasilitas pelayanan kesehatan diwajibkan untuk mengimplementasikan rekam medis elektronik selambat-lambatnya pada 31 Desember 2023. Ketentuan tersebut mendorong setiap fasilitas kesehatan untuk melakukan transformasi digital dalam sistem pencatatan medisnya, sebagai upaya menjaga kualitas dan efektivitas pelayanan kesehatan.

Implementasi rekam medis elektronik memiliki tantangan tersendiri. Jika risiko-risiko tersebut ditangani secara tepat, rumah sakit bisa menjamin keamanan pasien dan membuat sistem informasi rumah sakit berjalan lebih maksimal. [3]. Tantangan dalam melaksanakan RME sangatlah rumit, sehingga perlu dilakukan persiapan pra implementasi RME. Melalui evaluasi kesiapan ini, dapat diidentifikasi prosedur-prosedur yang dibutuhkan dan ditentukan skala prioritasnya, serta didukung pembentukan fungsi operasional yang tepat, guna memastikan pemanfaatan RME di institusi kesehatan berjalan secara optimal. [4]. Dengan demikian, selain

evaluasi kesiapan yang matang, pengelolaan risiko secara sistematis menjadi kunci keberhasilan implementasi RME untuk memastikan sistem dapat berjalan dengan optimal dan aman bagi pasien.

Organisasi yang mengandalkan teknologi informasi dituntut memiliki manajemen risiko yang mumpuni serta menjamin stabilitas sistem guna mencegah gangguan operasional yang dapat memicu kerugian [5]. Kegagalan dalam sistem RME memberikan dampak yang luas, bukan hanya menghambat efisiensi operasional dan merugikan pasien secara langsung melainkan juga dapat menurunkan tingkat kepercayaan masyarakat terhadap rumah sakit serta mengancam reputasi lembaga layanan kesehatan [6]. Dengan demikian, penerapan metode analisis risiko yang terstruktur menjadi langkah strategis dalam meminimalkan potensi kegagalan dan memastikan sistem RME dapat berjalan optimal guna mendukung terciptanya ekosistem kesehatan yang aman, berkualitas, dan memiliki tingkat kepercayaan publik yang tinggi. Manajemen risiko merupakan serangkaian aktivitas sistematis yang mencakup identifikasi potensi risiko, penilaian dampak dan kemungkinan terjadinya, pengendalian melalui strategi mitigasi yang tepat, serta upaya meminimalkan konsekuensi negatif yang dapat mempengaruhi seluruh aspek operasional organisasi kesehatan [7]. Guna meminimalisir potensi kegagalan dalam penerapan RME, fasilitas kesehatan perlu mengadopsi kerangka manajemen risiko yang terstruktur untuk mendeteksi, mengkaji, serta menanggulangi setiap kendala yang mungkin muncul saat implementasi RME. Dalam penerapan rekam medis elektronik, dapat timbul risiko akibat kesalahan dalam penggunaannya. Beberapa contohnya termasuk koneksi sistem, kerusakan atau masalah perangkat keras, jaringan yang tidak berfungsi, kegagalan cadangan data, pemadaman listrik, penyalahgunaan hak akses, kejahatan *siber*, dan lain-lain [8]. Terdapat tiga aspek penting yang menjadi ruang lingkup keamanan sistem informasi, yakni kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*).

Failure Mode and Effect Analysis (FMEA) merupakan cara konvensional yang dipilih untuk mengukur tingkat risiko terjadinya kegagalan dengan mengevaluasi tiga parameter utama. Parameter pertama adalah *Severity* (S) yang mengukur tingkat keparahan dampak dari suatu kegagalan, parameter kedua adalah *Occurrence* (O) yang menilai frekuensi atau kemungkinan terjadinya suatu kegagalan, dan parameter ketiga adalah *Detection* (D) yang mengukur kemampuan untuk mendeteksi kegagalan sebelum menimbulkan dampak [9]. Data yang telah dikumpulkan selanjutnya dianalisis menggunakan metode *Risk Priority Number* (RPN). Nilai RPN dihitung berdasarkan formula $RPN = S \times O \times D$, yaitu hasil perkalian antara tingkat keparahan (*Severity*), tingkat kejadian (*Occurrence*), dan tingkat deteksi (*Detection*). Berdasarkan hasil perhitungan RPN, dilakukan perankingan untuk mengidentifikasi prioritas risiko [10]. Risiko-risiko yang memiliki nilai RPN tertinggi akan dijadikan fokus utama dalam pelaksanaan upaya mitigasi dan perbaikan.

Berdasarkan hasil studi pendahuluan yang dilakukan di rumah sakit, potensi kegagalan pada data yakni adanya duplikasi nomor rekam medis pada bulan Januari - Maret terdapat 7 rekam medis dari 2287 pasien yang terdaftar atau setara dengan 0,03%, permasalahan ini dipicu oleh faktor pasien yang tidak membawa kartu identitas dan mengaku belum pernah berobat sebelumnya, permasalahan ini diketahui pada saat kunjungan kedua pasien. Keterlambatan deteksi ini berisiko terhadap keselamatan pasien, karena dikhawatirkan pada kunjungan pertama pasien memiliki alergi terhadap obat dan dokter tidak bisa mengakses riwayat pasien terdahulu, sehingga bisa menjadi peluang terjadinya kesalahan tindakan medis. Sejalan dengan penelitian [11] Ketepatan dalam identifikasi pasien merupakan tahap awal pelayanan yang sangat

menentukan dalam memitigasi risiko klinis serta memastikan efektivitas implementasi protokol keselamatan pasien.

Ditemukan adanya pengisian yang data yang tidak konsisten pada pendaftaran pendaftaran pada periode Januari - Maret 2026, dimana petugas yang mengisi rekam medis dengan tanda (-) pada beberapa kolom identitas pasien seperti, kolom agama 7,2% , pekerjaan 17,4%, penanggung jawab 32,5%, nama ibu 69,8%, tempat lahir 3,66%, golongan darah 99,4%, umur 79,4%, no telfon 11,4% yang sering kali tidak diisi. Alasan petugas menggunakan tanda tersebut untuk mempercepat proses pendaftaran dan penyimpanan data agar data bisa disimpan sementara. namun hal ini dapat berdampak pada pada kualitas data rekam medis. RME yang ada saat ini belum dilengkapi dengan fitur peringatan otomatis apabila terdapat komponen rekam medis yang belum terisi atau pengisiannya tidak sesuai dengan regulasi yang berlaku. Hal ini dapat berpotensi data menjadi tidak lengkap dan tidak akurat. Sejalan dengan penelitian [12] bahwasanya terjadinya duplikasi rekam medis dan ketidakkonsistenan pengisian rme termasuk dalam manajemen risiko pada kegagalan data.

Dengan demikian, peneliti tertarik melakukan penelitian tentang “Analisis Manajemen Risiko Pada Rekam Medis Elektronik Rawat Jalan Studi di Rumah Sakit Menggunakan Metode *Failure Mode And Effect Analysis* (FMEA)

II. METODE

Penelitian ini menggunakan metode deskriptif dengan pendekatan studi kasus di RSUD 'Aisyiyah Siti Fatimah Tulangan, yang dilaksanakan selama tiga bulan (April–Juni 2026), dengan menerapkan metode *Failure Mode and Effect Analysis* (FMEA). Sampel penelitian sebanyak 73 petugas rawat jalan (pendaftaran, poli, farmasi, radiologi, dan kasir) diambil menggunakan teknik total sampling, dengan instrumen berupa kuesioner serta teknik pengumpulan data melalui wawancara dan observasi langsung terhadap proses penggunaan Rekam Medis Elektronik (RME). Penelitian dilakukan melalui lima tahapan, yaitu observasi lapangan, identifikasi modus kegagalan, pengolahan data (penilaian skor *Severity*, *Occurrence*, dan *Detection*), analisis FMEA dengan perhitungan *Risk Priority Number* ($RPN = S \times O \times D$), hingga penyusunan rekomendasi mitigasi berdasarkan standar ISO/IEC 27001:2022 berdasarkan hasil perbandingan nilai RPN tertinggi.

III. Hasil dan Pembahasan

Manajemen Risiko RME rawat jalan menggunakan metode FMEA

a. Identifikasi Potensial *Failure Mode*

Tahapan dalam penilaian manajemen risiko menggunakan metode FMEA merupakan instrumen evaluasi risiko sistematis yang dirancang untuk mendeteksi berbagai potensi kegagalan dalam suatu alur proses, desain produk, maupun kinerja sistem, kemudian menilai dampaknya untuk menentukan prioritas mitigasi. Tahapan awal yaitu identifikasi kegagalan (*failure mode*). *Failure mode* merupakan bentuk atau cara terjadinya kegagalan pada suatu komponen, proses, atau sistem, sehingga fungsinya tidak dapat berjalan sebagaimana mestinya.

Berdasarkan data yang diperoleh melalui wawancara dengan pihak-pihak yang terlibat dalam operasional Rekam Medis Elektronik (RME) di rumah sakit, teridentifikasi beberapa aspek yang berpotensi mengalami kegagalan dan dapat memengaruhi kelancaran penyelenggaraan pelayanan kesehatan. Aspek tersebut meliputi data yang diinput ke dalam sistem rekam medis elektronik sebagai dasar pengelolaan informasi pasien, jaringan komunikasi

yang menghubungkan berbagai unit pelayanan sehingga mendukung pertukaran data secara terintegrasi, server sebagai media penyimpanan data terpusat yang dapat diakses oleh pengguna sesuai hak akses yang dimiliki, perangkat laptop atau komputer (PC) yang digunakan oleh pengguna dalam mengoperasikan sistem RME, serta layanan teknologi informasi yang bertanggung jawab dalam pengelolaan pengguna dan memastikan sistem rekam medis elektronik dapat beroperasi secara optimal [8].

Tabel 4. 1 Potensial Failure Mode pada RME Rawat Jalan di RS RSU ‘Aisysyah siti Fatimah Tulangan

No	Risiko	Akibat / Dampak
a. Potensi kegagalan Data		
1.	Data duplikasi	Kebingungan identitas
2.	Data tidak konsisten	Keputusan klinis tidak optimal
3.	<i>Human error</i> (salah input)	Kehilangan riwayat medis penting
4.	Data terhapus tidak sengaja oleh <i>user</i>	kehilangan riwayat medis penting
b. Potensi Kegagalan Jaringan		
1.	Gangguan teknis (Access Point) tidak bisa terhubung ke jaringan rumah sakit	Data tidak <i>real time</i>
2.	Iklan mengganggu dan menurunkan performa sistem	Iklan mengganggu dan menurunkan performa sistem
3.	Akun petugas dibobol	Pembobolah <i>username</i> dan <i>password</i>
c. Potensi kegagalan Teknologi		
1.	Tidak adanya fitur <i>log out</i> otomatis	Penyalahgunaan akun oleh orang lain
2.	Kurangnya personil IT	Pelayanan terganggu dan gangguan tidak segera ditangani
3.	Kurangnya kecepatan respons vendor	Terhambatnya kebutuhan user
d. Potensi Kegagalan Server		
1.	<i>Server down/crash</i>	RME tidak dapat di akses
e. Potensi Kegagalan Laptop / PC		
1.	Webcam tidak berfungsi	Tidak bisa verifikasi wajah
2.	Kegagalan wifi adapter menghambat koneksi wireless ke jaringan	Tidak bisa koneksi wireless
3.	RAM yang tidak mencukupi	Aplikasi lambat atau <i>crash</i>

4. User profile rusak

Pengguna tidak bisa *log in*

Berdasarkan tabel 4.2 Potensial Failure Mode pada RME Rawat Jalan di RSU 'Aisyiyah Siti Fatimah Tulangan bahwa teridentifikasi beberapa potensi kegagalan pada setiap komponen sistem. Pada komponen data, potensi kegagalan meliputi duplikasi data, ketidakkonsistenan data, dan *human error* berupa kesalahan input. Pada komponen jaringan, potensi kegagalan yang ditemukan meliputi gangguan teknis berupa *access point* yang tidak dapat terhubung ke jaringan rumah sakit, munculnya iklan yang mengganggu dan menurunkan performa sistem, serta pembobolan akun petugas. Sementara itu, pada komponen layanan teknologi informasi, potensi kegagalan meliputi tidak tersedianya fitur *logout* otomatis, keterbatasan jumlah personel teknologi informasi, dan lambatnya respons dari vendor. Pada komponen server, potensi kegagalan yang teridentifikasi adalah *server down* atau *crash*. Adapun pada komponen laptop atau PC, potensi kegagalan meliputi webcam yang tidak berfungsi, kegagalan *Wi-Fi adapter* yang menghambat koneksi ke jaringan nirkabel, serta kerusakan pada *user profile*.

b. Menganalisis penyebab dan akibat dari masing-masing bentuk kegagalan yang teridentifikasi pada sistem RME rawat jalan di RSU 'Aisyiyah Siti fatimah Tulangan

Tahapan kedua dalam melakukan penilaian / manajemen risiko menggunakan metode FMEA adalah analisis penyebab dan akibat dari masing-masing bentuk kegagalan. Analisis penyebab dan akibat dari masing-masing bentuk kegagalan dalam FMEA merupakan proses untuk mengidentifikasi faktor-faktor yang menyebabkan suatu kegagalan terjadi serta menilai dampak yang ditimbulkan terhadap sistem, proses, atau layanan [13] Berikut merupakan hasil wawancara terkait sebab dan akibat dari bentuk kegagalan RME rawat jalan di RSU 'Aisyiyah Siti fatimah Tulangan.

Tabel 4. 2 Analisis penyebab dan akibat dari masing-masing bentuk kegagalan yang teridentifikasi pada sistem RME rawat jalan di RSU 'Aisyiyah Siti fatimah Tulangan

No	Risiko	Penyebab	Upaya
a. Potensi kegagalan Data			
1.	Data duplikasi	Pasien tidak membawa kartu identitas atau mengaku belum pernah berobat sebelumnya	Petugas harus lebih teliti dalam identifikasi pasien di awal pelayanan
2.	Data tidak konsisten	Petugas menggunakan tanda (-) untuk mempercepat proses pendaftaran	Penambahan fitur peringatan otomatis (<i>automatic warning</i>) jika ada kolom yang belum terisi
3.	Human error (salah input)	Kesalahan petugas saat memasukkan	Pelatihan rutin bagi petugas mengenai

No	Risiko	Penyebab	Upaya
		data	pengisian RME secara akurat
4.	Data terhapus tidak sengaja oleh <i>user</i>	saling meminjam <i>username</i> dan <i>password</i>	Penerapan kebijakan larangan berbagi <i>username</i> dan <i>password</i> antartugas
b. Potensi Kegagalan Jaringan			
1.	Gangguan teknis (Access Point) tidak bisa terhubung ke jaringan rumah sakit	Perangkat acces point mengalami gangguan teknis	Pemeliharaan jaringan berkala
2.	Iklan mengganggu dan menurunkan performa sistem	Log in SIMRS Khanza menggunakan web	Menggunakan aplikasi dekstop SIMRS Khanza
3.	Akun petugas dibobol	Petugas berbagi <i>username</i> dan <i>password</i>	Penguatan sistem keamanan <i>siber</i>
c. Potensi kegagalan Teknologi			
1.	Tidak adanya fitur logout otomatis	SIMRS Khanza belum dilengkapi fitur logout otomatis	Evaluasi pengaturan sistem untuk menambahkan fitur <i>logout</i> otomatis.
2.	Kurangnya personil IT	Keterbatasan sumber daya manusia	Penambahan jumlah staf IT atau peningkatan respon teknis.
3.	Kurangnya kecepatan respons vendor	SIMRS khanza opensource	Kebutuhan pengguna sistem (<i>user</i>) menjadi terhambat
d. Potensi Kegagalan Server			
1.	Server down/crash	Beban server tinggi	<i>Maintenance server</i> rutin dan <i>backup data</i>
e. Potensi Kegagalan Laptop / PC			
1.	Webcam tidak berfungsi	Webcam belum terpasang dengan baik	Pengecekan dan perbaikan ulang perangkat keras webcam
2.	Kegagalan wifi adapter menghambat koneksi wireless ke jaringan	Kerusakan pada modul wifi adapter perangkat pc	Perbaikan atau penggantian modul WiFi.
3.	RAM yang tidak	Spesifikasi RAM	<i>Upgrade</i> kapasitas

No	Risiko	Penyebab		Upaya
	mencukupi	perangkat penuh	hampir	memori (RAM) perangkat.
4.	User profile rusak	Kerusakan pengguna dimatikan paksa	file akibat secara	Perbaikan profil pengguna oleh tim IT.

Berdasarkan tabel 4.3 Analisis penyebab dan akibat dari masing-masing bentuk kegagalan yang teridentifikasi pada sistem RME rawat jalan di RSUD ‘Aisyiyah Siti fatimah Tulangan yang dikelompokkan ke dalam lima kategori utama, yakni potensi kegagalan pada aspek data, jaringan, teknologi informasi (IT), server, serta perangkat keras berupa laptop atau PC.

Pada kategori data, permasalahan utama seperti duplikasi identitas dan input data yang tidak konsisten, *human error* dan data terhapus tidak sengaja sering disebabkan oleh ketidaktepatan petugas maupun kebiasaan pasien yang tidak membawa kartu identitas dan seringnya petugas menggunakan username password milik rekan kerjanya. Sehingga diperlukan upaya yang harus dilakukan adalah meningkatkan ketelitian petugas. Menambah fitur peringatan otomatis (*automatic warning*), serta mengadakan pelatihan rutin kepada petugas. Pada aspek sistem dan teknologi informasi, tabel tersebut menyoroti keterbatasan fitur pada SIMRS Khanza, seperti ketiadaan fungsi *log out* otomatis, serta kendala sumber daya manusia berupa kurangnya personil IT.

Sebagai sistem berbasis *open source*, dan respons vendor yang lambat turut menjadi hambatan yang dapat mengganggu pemenuhan kebutuhan pengguna sehingga pengguna harus menunggu lama untuk pemenuhan kebutuhan. Meskipun aplikasi SIMRS Khanza telah tersedia dalam versi desktop, petugas lebih memilih mengaksesnya melalui web dikarenakan tampilan pada versi desktop dinilai terlalu kecil, baik dari segi ukuran layar maupun teks, sehingga menyulitkan saat digunakan. Sementara itu, akses melalui web dianggap lebih fleksibel karena ukuran tampilannya dapat disesuaikan sesuai kebutuhan pengguna. Pada aspek server, risiko yang muncul berupa potensi gangguan (*down* atau *crash*) apabila beban kerja sistem terlalu tinggi upaya yang dilakukan adalah perlu dilakukannya pemeliharaan server dan *backup* data secara rutin. Pada aspek perangkat keras, risiko yang teridentifikasi meliputi kegagalan fungsi kamera web, kerusakan modul WiFi, serta kapasitas RAM yang tidak memadai untuk menjalankan aplikasi. Untuk mengatasi berbagai risiko tersebut mengusulkan langkah mitigasi mulai dari pemeliharaan rutin dan perbaikan perangkat keras, penambahan fitur peringatan otomatis, hingga pelatihan bagi staf.

c. Menganalisis tingkat risiko terhadap setiap bentuk kegagalan berdasarkan parameter *Severity* (S), *Occurrence* (O), dan *Detection* (D) dan RPN.

Berdasarkan risiko-risiko yang telah teridentifikasi, tahap selanjutnya adalah menilai setiap risiko dari tiga aspek, yaitu tingkat keparahan (*severity*), tingkat keseringan terjadinya (*occurrence*), dan tingkat kemudahan mendeteksi (*detection*), menggunakan skala 1 sampai 10. Semakin tinggi skor yang diberikan, semakin besar tingkat keparahan, semakin sering risiko terjadi, atau semakin sulit risiko tersebut dideteksi. Penilaian ini diberikan oleh masing-masing responden untuk setiap potensi kegagalan yang telah teridentifikasi. Karena setiap responden dapat memberikan skor yang berbeda, maka untuk memperoleh satu nilai yang mewakili seluruh responden, skor yang diberikan pada setiap aspek dijumlahkan lalu dirata-ratakan. Misalnya,

pada risiko data duplikasi, seluruh skor *severity* dari responden dijumlahkan kemudian dibagi dengan jumlah responden untuk memperoleh nilai rata-rata *severity*, cara yang sama dilakukan untuk *occurrence* dan *detection*. Ketiga nilai rata-rata tersebut kemudian dikalikan untuk memperoleh nilai *Risk Priority Number* (RPN) dari setiap risiko, sehingga dapat diketahui risiko mana yang memiliki prioritas tertinggi hingga terendah, dengan rumus:

$$RPN = S \times O \times D.$$

Tabel 4. 3 Analisis tingkat risiko dari setiap bentuk kegagalan berdasarkan parameter *Severity* (*S*), *Occurrence* (*O*), dan *Detection* (*D*)

No	risiko	Severity	Occurance	Detection	RPN	Kategori
a. Potensi kegagalan Data						
1.	Data duplikasi	8	6	4	192	Very High
2.	Data tidak konsisten	6	6	5	180	Very High
3.	Human error (salah input)	6	5	4	120	High
4.	Data terhapus tidak sengaja oleh user	6	3	2	36	Low
b. Potensi Kegagalan Jaringan						
1.	Gangguan teknis (Access Point) tidak bisa terhubung ke jaringan rumah sakit	5	4	2	40	Low
2.	Iklan mengganggu dan menurunkan performa sistem	7	5	2	70	Medium
3.	Akun petugas dibobol	6	4	2	48	Low
c. Potensi kegagalan Teknologi						
1.	Tidak adanya fitur logout otomatis	8	7	3	168	Very High
2.	Kurangnya personil IT	7	6	2	84	Medium
3.	Kurangnya kecepatan respons vendor	7	4	2	56	Medium
d. Potensi Kegagalan Server						
1.	<i>Server down/crash</i>	7	7	2	98	Medium
e. Potensi Kegagalan Laptop / PC						
1.	Webcam tidak berfungsi	5	5	2	50	Low
2.	Kegagalan wifi adapter menghambat koneksi wireless ke jaringan	6	4	2	48	Low
3.	RAM yang tidak mencukupi	4	3	3	36	Low
4.	<i>User profile</i> rusak	2	2	2	8	Very Low

d. Klasifikasi Risiko

Klasifikasi risiko adalah tahapan pengelompokan risiko berdasarkan tingkat dampak yang ditimbulkan dan frekuensi terjadinya [14]. Seluruh risiko kemudian diurutkan berdasarkan nilai RPN, dari yang tertinggi sampai terendah, yang mana nilai tersebut dihasilkan dari perkalian antara tingkat keparahan (*severity*), kejadian (*occurrence*), dan deteksi (*detection*).

Tabel 4. 4 Klasifikasi Risiko

Skala	Level
>151	Very Hight
101 - 150	Hight
51 - 100	Medium
20 - 50	Low
0-19	Very Low

Berdasarkan hasil klasifikasi risiko pada Tabel 4.4, diketahui bahwa hasil RPN tertinggi berada pada level *very high* dengan skor 192, yaitu pada risiko duplikasi data, sedangkan nilai RPN terendah berada pada level *very low* dengan skor 8, yaitu pada risiko *user profile* yang rusak. Hasil penilaian risiko ini dikelompokkan ke dalam lima tingkatan, yaitu sangat tinggi, tinggi, sedang, rendah, dan sangat rendah, guna memudahkan penentuan prioritas penanganan berdasarkan besar-kecilnya nilai RPN yang diperoleh. Rincian hasil perhitungan RPN untuk masing-masing risiko.

- Level *very high* memiliki 3 risiko jika antara RPN >150
- Level *high* memiliki 1 risiko jika RPN antara 101 - 150
- Level *medium* memiliki 4 risiko jika RPN antara 51 - 100
- Level *Low* memiliki 6 risiko jika RPN antara 20 - 50
- Level *very low* memiliki 1 risiko jika RPN antara 0 – 19

Tabel 4. 5 *Matrix* Penilaian Manajemen Risiko

Level kemungkinan	Level Dampak				
	Tidak signifikan	Minor	medium	signifikan	Sangat signifikan
Sangat besar		50	98	192	
Besar		48	84	120	180
Sedang	36	48	70		168
Kecil		40	56		
Sangat kecil	8	36			

Matriks risiko merupakan alat bantu visual yang penting dalam proses identifikasi, analisis, dan pengelolaan risiko sistem informasi secara lebih terstruktur [15]. Melalui *matriks* risiko yang disajikan pada tabel 4.6, rumah sakit dapat meningkatkan kesiapsiagaan dalam menghadapi berbagai ancaman terhadap sistem informasi serta menentukan prioritas langkah mitigasi yang tepat guna melindungi data pasien yang bersifat sensitif.

Tabel 4.6 Level Risiko

Level Risiko	Rentang Besara Risiko	Simbol Warna
Sangat kecil	1 – 19	Biru
Kecil	20 – 50	Hijau
Sedang	51 – 100	Kuning
Besar	101 – 150	Jingga
Sangar besar	>151	Merah

Tujuan identifikasi risiko adalah untuk menjadi dasar dalam menentukan langkah dan kebijakan yang tepat, agar risiko dapat dicegah, ditangani, serta dampaknya bisa diminimalkan. Upaya meminimalisir dampaknya melalui upaya mitigasi yang sesuai dengan standar ISO/IEC 27001:2022."

Mitigasi Risiko Menggunakan ISO /IEC 27001:2022

Mitigasi risiko adalah langkah strategis yang diambil untuk mengurangi peluang terjadinya ancaman atau memperkecil dampak negatif yang timbul jika risiko tersebut terjadi. Tahap ini bertujuan untuk menyusun rekomendasi manajemen risiko dengan mengacu pada hasil prioritas risiko yang telah diperoleh melalui perhitungan nilai RPN sebelumnya. Penentuan prioritas difokuskan pada risiko-risiko yang berada pada level *very high*. mengingat

kategori tersebut berpotensi menimbulkan kerugian yang cukup besar serta dapat mengganggu kelangsungan proses bisnis yang sedang berjalan apabila tidak segera ditangani.

Tabel 4. 7 Mitigasi Risiko

Level	Risiko	Potensi kegagalan	Sev	Occ	Det	RPN
Very high	Data duplikasi	Kebingungan identitas	8	6	4	192
Very high	Data tidak konsisten	Keputusan klinis tidak optimal	6	6	5	180
Very high	Tidak ada fitur <i>log out</i> otomatis	Penyalahgunaan akun	6	5	4	168

Berdasarkan hasil perangkingan nilai RPN pada tabel 4.8, rekomendasi mitigasi disusun dengan mengacu pada kontrol keamanan informasi dalam ISO/IEC 27001:2022. Fokus mitigasi diarahkan pada keempat risiko dengan kategori *Very High*.

Tabel 4. 8 Mitigasi Risiko ISO/IEC 27001:2022

No	Prioritas Risiko (RPN)	Kontrol ISO/IEC 27001:2022	Rekomendasi Mitigasi
1.	Data duplikasi (RPN 192 – <i>Very High</i>)	A.6.3 kesadaran, edukasi, dan pelatihan keamanan informasi. A.5.33 perlindungan rekaman	Pelatihan berkala kepada petugas pendaftaran mengenai identifikasi data pasien. Mengaktifkan fitur pencarian / pencocokan data otomatis pada simrs.
2.	Data tidak konsisten (RPN 180 – <i>Very High</i>)	A.5.33 Perlindungan catatan A.8.9 Manajemen konfigurasi A.8.28 Rekayasa perangkat lunak yang aman	Menambahkan validasi isian wajib (mandatory field) dan fitur peringatan otomatis (automatic warning) pada sistem sebelum data dapat disimpan. Melakukan audit kelengkapan data rekam medis. Menyusun kebijakan formal yang melarang penggunaan tanda “-“ tanpa keterangan yang sah
3.	Tidak ada fitur <i>log out</i> otomatis (RPN 168 – <i>Very High</i>)	A.8.5 Autentikasi yang aman A.5.15 Kontrol akses	Melakukan konfigurasi fitur <i>auto-logout</i> yang akan aktif setelah periode tertentu

tanpa aktivitas aplikasi Khanza. Selain itu, organisasi juga menyusun peraturan sebagai upaya mengontrol akses terhadap sistem dan aplikasi.	adanya pada SIMRS
--	-------------------

V. SIMPULAN

Penelitian ini bertujuan untuk menganalisis manajemen risiko dalam implementasi Rekam Medis Elektronik (RME) di unit rawat jalan dengan menerapkan metode *Failure Mode and Effect Analysis* (FMEA). Berdasarkan hasil analisis, ditemukan empat risiko utama yang menempati kategori *Very High* berdasarkan nilai *Risk Priority Number* (RPN) tertinggi, yaitu duplikasi data (192), ketidakkonsistenan pengisian data (180), ketiadaan fitur *auto-logout* (168), dan kesalahan manusia. Masalah-masalah tersebut diidentifikasi dari faktor ketidaktelitian petugas dalam proses pendaftaran, penggunaan karakter non-informatif untuk mempercepat input, serta keterbatasan fitur keamanan sistem yang berpotensi mengancam integritas dan kerahasiaan data pasien.

Sebagai langkah penanggulangan, strategi mitigasi disusun menggunakan standar ISO/IEC 27001:2022 guna memastikan stabilitas operasional dan keamanan informasi medis. Rekomendasi perbaikan mencakup aspek teknis seperti penerapan fitur validasi (*mandatory field*) dan peringatan otomatis, serta konfigurasi *log out* otomatis untuk mencegah akses tidak sah. Selain itu, Penguatan aspek sumber daya manusia melalui pelatihan rutin mengenai tata kelola RME dan pemberlakuan kebijakan ketat terkait larangan berbagi akun akses menjadi hal yang sangat penting dalam meminimalisir risiko kegagalan sistem.

UCAPAN TERIMA KASIH

Terima kasih kepada dosen pembimbing atas arahan, saran, dan kritik yang membangun. Terima kasih juga kepada peneliti terdahulu atas karya yang menjadi referensi penting dalam kajian analisis manajemen risiko menggunakan metode FMEA. Dukungan, semangat, dan doa dari keluarga, sahabat, serta rekan sejawat menjadi kekuatan besar dalam penyelesaian artikel ini.

REFERENSI

- [1] M. K. Maha Wirajaya and N. Made Umi Kartika Dewi, “Analisis Kesiapan Rumah Sakit Dharma Kerti Tabanan Menerapkan Rekam Medis Elektronik,” *J. Kesehat. Vokasional*, vol. 5, no. 1, p. 1, Feb. 2020, doi: 10.22146/jkesvo.53017.
- [2] menteri kesehatan, *Permenkes No. 24*. 2022.
- [3] E. Simanjuntak, A. S. Hasibuan, S. P. S. Lubis, S. K. Karo, Z. Ritonga, and D. Hulu, “ANALISIS PENERAPAN MANAJEMEN RESIKO PADA REKAM MEDIS ELEKTRONIK DI UPT PUSKESMAS KOTA MATSUM,” 2025.
- [4] E. W. Faida and A. Ali, “Analisis Kesiapan Implementasi Rekam Medis Elektronik dengan Pendekatan DOQ-IT (Doctor’s Office Quality-Information Technology),” *J. Manaj. Inf. Kesehat. Indones.*, vol. 9, no. 1, p. 67, Mar. 2021, doi: 10.33560/jmiki.v9i1.315.
- [5] K. P. Ningsih, U. Tunnisa, and N. Erviana, “Manajemen Resiko Redesign Sistem Penjajaran Rekam Medis dengan Metode Failure Mode and Effect Analysis (FMEA),” 2020.
- [6] U. S. Suhariyono, F. R. Ikawati, and N. Afifah, “Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso,” vol. 13, no. 1, 2025.
- [7] Priyo DanuUkito, “MANAJEMEN RISIKO PADA BAGIAN PENYIMPANAN REKAM MEDIS DI RSUD dr. SOEDIRAN MANGUN SUMARSO WONOGIRI.” 2025.
- [8] Y. Ramayani and T. Oktarina, “Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA).” 2022.
- [9] B. Mustofa, E. Paranita, and T. Sukwika, “Manajemen Risiko Dengan Metode FMEA di Instalasi Gawat Darurat Rumah Sakit Kuwait.pdf.” 2023.
- [10] Rizqi Aulia husna1, Eka Rahma Ningsih1*, “RISIKO PADA REKAM MEDIS ELEKTRONIK RAWAT INAP MENGGUNAKAN METODE FMEA DI RUMAH SAKIT ISLAM BANJARMASIN.pdf.” 2025.
- [11] A. Kristijono, P. R. prabowo, anggun Tiara, and M. irfan fatoni, “Tahapan Metode Failure Mode Effect and Analysis (FMEA) dalam Analisis Risiko RME.” 2025.
- [12] A. Jaelani Rusdi, N. P. Reni Mahyuni, and S. Nada Ayunani Cininta, “Manajemen Kelengkapan Catatan Medis (KLPCM) di Rekam Medis Elektronik Rumah Sakit Tk. II Udayana.” 2024.
- [13] M. Ramadan, R. Fitriani, and Sukanta, “Analisis Kesehatan Dan Keselamatan Kerja Menggunakan Failure Mode And Effect Analysis Di PT. XYZ,” vol. 23, 2021.
- [14] mu’adzah and N. A. Firmansyah, “Analisis Enterprise Risk Management Menggunakan FMEA pada PT XYZ.” *Teknoin*, 2020.
- [15] filany cahya arumdiya and christ rudianto, “Implementasi ISO 27001:2022 dalam Manajemen Risiko Keamanan Informasi.” *Jurnal PETISI*, 2025.

Conflict of Interest Statement:

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.