Jurnal Praba : Jurnal Rumpun Kesehatan Umum
Volume. 4, Nomor. 3, September 2026
e-ISSN :3030-8283 ; p-ISSN :3030-8828, Hal. 240-253
DOI: https://doi.org/10.62027/praba.v4i3.974
Tersedia: https://journal.stikescolumbiasiamdn.ac.id/index.php/Praba

Analisis Risiko Kebocoran Data Pasien dan Upaya Pencegahan pada Rekam Medis Elektronik di Rumah Sakit X

Bella Qianti Putri Zahira [1*], Diansyah [2]
[1,2] Rekam Medis dan Informasi Kesehatan, Politeknik Piksi Ganesha, Indonesia
Email: bellazahira24@gmail.com[1], diansyahrm1@gmail.com[2]

[*]*Penulis Korespondensi : bellazahira24@gmail.com*

Abstract*. The implementation of electronic medical records improves healthcare service efficiency but also presents challenges related to patient data security and confidentiality. This study aimed to analyze the risks of patient data breaches and preventive measure for electronic medical records at Hospital X. A descriptive qualitative approach was employed, with data collected through in-depth interviews, observations, and document reviews. The findings showed that no official reports of patient data breaches had been identified however, several risks remained, including audit trail monitoring that was not conducted regularly, access rights not fully aligned with user's roles, the absence of two-factor authentication, inactive automatic logout, cloud storage still under consideration, and human error. The study concludes that EMR security still needs to be strengthened. EMR security is recommended to receive continuous strengthening through improvements in technology, policies, monitoring, and user awareness. Strengthening policies, incident response procedures, and user training, as well as fostering a security-conscious culture, are also essential to safeguarding the confidentiality, integrity, and availability of patient data. These measures are expected to prevent security incidents while enhancing patient trust in the hospital's healthcare services.*

Keywords: *Cloud Storage; Data Breaches; EMR; Information Security; Risk Manajement.*

Abstrak. Penerapan rekam medis elektronik memberikan manfaat dalam meningkatkan efisiensi pelayanan kesehatan, namun juga menghadirkan tantangan terkait keamanan dan kerahasiaan data pasien. Penelitian ini bertujuan menganalisis risiko kebocoran data pasien serta upaya pencegahannya pada rekam medis elektronik di Rumah Sakit X. Penelitian menggunakan pendekatan kualitatif deskriptif dengan data yang diperoleh melalui wawancara mendalam, observasi, dan telaah dokumen. Hasil penelitian menunjukkan belum terdapat laporan resmi mengenai kebocoran data pasien, namun masih terdapat risiko berupa pemantauan audit trail yang belum dilakukan secara berkala, pengaturan hak akses yang belum sepenuhnya disesuaikan dengan peran pengguna, belum diterapkannya *two-factor authentication*, belum aktifnya kembali fitur logout otomatis, *cloud storage* yang masih dalam tahap kajian, serta faktor human error. Simpulan penelitian menunjukkan bahwa keamanan RME masih perlu diperkuat. Keamanan RME disarankan mendapat penguatan yang berkelanjutan melalui peningkatan aspek teknologi, kebijakan, pengawasan, serta kesadaran pengguna. Penguatan kebijakan, prosedur respons insiden, pelatihan pengguna, serta peningkatan budaya sadar keamanan juga diperlukan untuk menjaga kerahasiaan, integritas, dan ketersediaan data pasien. Langkah tersebut diharapkan mencegah insiden keamanan sekaligus meningkatkan kepercayaan pasien terhadap pelayanan kesehatan rumah sakit.

Kata Kunci: *Cloud Storage*; Keamanan Informasi; Kebocoran Data; Manajemen Risiko; RME.

1. PENDAHULUAN

Menurut Undang-Undang No. 17 Tahun 2023 tentang Kesehatan menyebutkan bahwa rumah sakit merupakan fasilitas pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perseorangan secara paripurna melalui pelayanan kesehatan promotif, preventif, rehabilitatif, dan/atau paliatif dengan menyediakan pelayanan rawat inap, rawat jalan, dan gawat darurat (Undang-Undang No. 17, 2023).

Naskah Masuk: 18 Juni 2026; Revisi: 19 Juli 2026; Diterima; 20 Agustus 2026; Terbit: 07 September 2026

Berdasarkan Peraturan Menteri Kesehatan No. 24 Tahun 2022 pasal 1 menyebutkan rekam medis merupakan dokumen yang berisikan data identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien. Selanjutnya pada pasal 3 ayat 1 setiap fasilitas pelayanan kesehatan wajib menyelenggarakan rekam medis elektronik (Permenkes No. 24, 2022). Implementasi Rekam Medis Elektronik (RME) juga sejalan dengan arah kebijakan transformasi digital kesehatan yang ditetapkan pemerintah dalam Peraturan Presiden No. 18 Tahun 2020 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024 pada dokumen tersebut, digitalisasi rekam medis dan pengembangan rekam medis online menjadi salah satu strategi nasional dalam meningkatkan mutu pelayanan kesehatan secara berkelanjutan. (Perpres No. 18, 2020).

Rekam medis elektronik berperan dalam meningkatkan efektivitas pelayanan melalui akses informasi yang lebih cepat, proses kerja yang lebih efisien, serta pelaksanaan tugas tenaga kesehatan yang lebih optimal (Tasbihah & Yunengsih, 2024). Berdasarkan Pasal 29 dalam Permenkes No. 24 Tahun 2022, penyelenggaraan rekam medis wajib menerapkan prinsip kerahasiaan *(confidentiality)*, integritas *(integrity)*, serta ketersediaan *(availability)*. Prinsip kerahasiaan bertujuan melindungi data pasien dari akses pihak yang tidak berwenang. Prinsip integritas memastikan data tetap akurat dan tidak mengalami perubahan tanpa izin, sehingga setiap perubahan dapat ditelusuri. Prinsip ketersediaan memastikan data dapat diakses oleh pihak yang berwenang ketika diperlukan (Listyorini & Sintya, 2021).

Pelindungan data pasien juga diperkuat melalui Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi yang menegaskan tanggung jawab fasilitas pelayanan kesehatan dan penyelenggaraan sistem elektronik untuk melindungi kerahasiaan serta hak privasi pasien dengan menerapkan langkah pengamanan yang memadai (Undang-Undang No. 27, 2022). Selain itu, pengelolaan keamanan informasi dapat mengacu pada standar ISO/IEC 27001 tentang *Information Security Management System* (ISMS). Standar tersebut menyediakan kerangka kerja dalam pengelolaan risiko keamanan informasi melalui pengendalian akses, pelindungan data, pengamanan sistem, pemantauan aktivitas pengguna, serta penanganan insiden keamanan. Penerapan standar tersebut penting untuk mencegah akses tidak sah, penyalahgunaan data, perubahan data tanpa izin, maupun kebocoran informasi pasien (Permana & Nuraeni, 2025).

Meskipun berbagai regulasi telah diterapkan, masalah pelanggaran data dalam sektor kesehatan Indonesia masih menjadi persoalan serius. Salah satu kejadian yang banyak mendapat sorotan adalah pelanggaran data pada tahun 2021 yang terjadi di BPJS Kesehatan, yang dilaporkan melibatkan lebih dari 279 juta catatan individu yang diasuransikan, termasuk

data diri, nomor KTP, alamat, nomor kontak, dan informasi kesehatan yang diperjualbelikan melalui platform digital. Insiden tersebut menunjukkan bahwa kebocoran data tidak hanya meliputi penyalahgunaan informasi pribadi dan kerugian individu yang terlibat, tetapi juga bisa menurunkan kepercayaan masyarakat terhadap institusi layanan kesehatan (Sorisa et al., 2024).

Beberapa penelitian sebelumnya telah mengidentifikasi berbagai faktor yang berkontribusi terhadap terjadinya risiko dan insiden kebocoran data rekam medis elektronik. Penelitian yang dilakukan oleh Riska Pradita, Retno Kusumo, dan Rahmawati pada tahun 2022 dengan judul Pentingnya Aspek Keamanan Informasi Data Pasien pada Penerapan RME di Puskesmas menunjukkan bahwa untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi dapat ditingkatkan melalui penggunaan akun pengguna yang bersifat individual, penerapan enkripsi, fitur *logout* otomatis, serta pelaksanaan pencadangan data secara berkala (Pradita et al., 2022). Penelitian oleh Santi Lestari, Sucipto, Nastiti Azizah pada tahun 2025 dengan judul Tinjauan Penerapan Sistem Informasi Rekam Medis Elektronik Terhadap Keamanan Data Pasien di Rumah Sakit Kartini Rangkasbitung menjelaskan bahwa pelindungan data pasien diterapkan melalui pengendalian hak akses dan mekanisme autentikasi berbasis akun. Namun, penelitian tersebut lebih berfokus pada evaluasi penerapan sistem dibandingkan identifikasi serta klasifikasi risiko kebocoran data secara mendalam. Selain itu, keterkaitan antara potensi kerentanan sistem dengan strategi pencegahan belum dianalisis secara menyeluruh sehingga analisis risiko yang disajikan masih terbatas (Lestari et al., 2025). Sementara itu, penelitian yang dilakukan oleh Untung Slamet Suhariyono, Fita Rusdian Ikawati, dan Nur Afifah pada tahun 2025 dengan judul Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso lebih berfokus pada evaluasi penerapan keamanan sistem kesehatan secara luas, sehingga belum secara spesifik membahas risiko kebocoran data serta strategi pencegahannya di rumah sakit. Oleh karena itu, identifikasi risiko dan evaluasi keamanan perlu dilakukan secara berkelanjutan (Suhariyono et al., 2025).

Rumah Sakit X telah menerapkan rekam medis elektronik pada seluruh unit pelayannya, yang meliputi pelayanan rawat jalan, rawat inap, dan instalasi gawat darurat. Penerapan rekam medis elektronik dilakukan untuk mendukung peningkatan mutu pelayanan, mempercepat proses akses informasi pasien, serta mempermudah integrasi data pelayanan kesehatan (Putra & Widyaningrum, 2025). Berdasarkan hasil wawancara pendahuluan dengan kepala unit rekam medis, ditemukan beberapa kondisi yang berpotensi menimbulkan risiko kebocoran data pasien, antara lain pemantauan *audit trail*, belum diterapkannya autentikasi dua faktor *(two factor authentication)*, belum aktifnya kembali fitur *logout* otomatis *(idle time)*, serta kebijakan

hak akses yang belum sepenuhnya disesuaikan dengan peran dan unit kerja pengguna. Selain itu, keamanan server *backup* dan sistem penyimpanan berbasis *cloud* masih memerlukan evaluasi untuk memastikan pelindungan data pasien.

Hasil wawancara juga menunjukkan bahwa akses SIMRS dari luar lingkungan rumah sakit masih memiliki potensi risiko keamanan apabila tidak didukung oleh mekanisme pengamanan yang memadai. Selain itu, pernah ditemukan kejadian petugas mendokumentasikan isi Catatan Perkembangan Pasien Terintegrasi (CPPT) dan mengirimkannya melalui media komunikasi untuk kepentingan koordinasi pelayanan. Meskipun tidak berkembang menjadi kasus kebocoran data yang dilaporkan secara resmi, kondisi tersebut menunjukkan adanya potensi pelanggaran kerahasiaan informasi pasien yang perlu mendapatkan perhatian dan pengendalian lebih lanjut. Berdasarkan kondisi tersebut, analisis risiko kebocoran data pada rekam medis elektronik perlu dilakukan untuk mengidentifikasi potensi kerentanan yang dapat mengancam keamanan informasi pasien. Oleh karena itu, penelitian ini bertujuan untuk menganalisis risiko kebocoran data serta upaya pencegahannya yang diterapkan pada rekam medis elektronik pasien di Rumah Sakit X.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif untuk menganalisis risiko kebocoran data dan upaya pencegahannya pada rekam medis elektronik pasien di Rumah Sakit X. Pendekatan kualitatif digunakan untuk memahami fenomena yang terjadi secara mendalam berdasarkan kondisi yang ada di lapangan melalui informasi yang diperoleh dari informan yang terlibat langsung dalam objek penelitian (Fiantika et al., 2022). Penelitian dilaksanakan di unit rekam medis Rumah Sakit X yang telah menerapkan sistem rekam medis elektronik. Periode penelitian berlangsung dari 1 April 2026 hingga 31 Mei 2026. Tujuan penelitian ini adalah mengidentifikasi potensi risiko kebocoran data rekam medis elektronik pasien serta mengevaluasi upaya pencegahan yang diterapkan oleh rumah sakit.

Data yang digunakan dalam penelitian ini terdiri dari data primer dan data sekunder. Data primer diperoleh melalui wawancara mendalam dan observasi langsung terhadap informan penelitian, sedangkan data sekunder diperoleh melalui telaah dokumen rumah sakit yang berkaitan dengan penerapan dan keamanan rekam medis elektronik. Penelitian ini melibatkan tujuh orang informan, karakteristik informan penelitian disajikan pada Tabel 1. Informan dipilih menggunakan teknik purposive sampling. Teknik purposive sampling digunakan untuk memilih sampel berdasarkan kriteria yang relevan dengan tujuan penelitian (Sugiyono, 2019).

Tabel 1. Karakteristik Informan.

Kode Informan	Jabatan	Unit Kerja
Informan 1	Kepala Instalasi Rekam Medis	Rekam Medis
Informan 2	Petugas Teknologi Informasi (IT)	IT
Informan 3	Petugas Rekam Medis	Rekam Medis
Informan 4	Petugas Rekam Medis	Rekam Medis
Informan 5	Dokter Spesialis Poliklinik	Instalasi Rawat Jalan
Informan 6	Perawat	Instalasi Rawat Jalan
Informan 7	Apoteker	Farmasi

Sumber: Data Primer Hasil Wawancara, 2026 (diolah)

Berdasarkan Teknik tersebut, informan dipilih karena memiliki keterlibatan langsung dalam penggunaan dan pengelolaan sistem rekam medis elektronik. Informan Kriteria inklusi dalam penelitian ini yaitu petugas yang memiliki pengalaman minimal satu tahun dalam penggunaan atau pengelolaan rekam medis elektronik, memahami prosedur pengelolaan data pasien, serta bersedia menjadi informan penelitian. Adapun kriteria eksklusi penelitian mencakup petugas yang sedang cuti, sakit, atau tidak aktif bertugas selama periode pengumpulan data, petugas yang sedang menjalani mutasi atau rotasi tugas sehingga tidak lagi menangani rekam medis elektronik saat penelitian berlangsung. Penelitian dilaksanakan melalui beberapa tahapan, yaitu identifikasi masalah, studi literatur, penyusunan instrumen penelitian, pengurusan izin penelitian, pengumpulan data, analisis data, dan penyusunan laporan penelitian.

Instrumen utama dalam penelitian ini adalah peneliti yang dibantu dengan pedoman wawancara, lembar observasi, *checklist* observasi (Fadli, 2021). Wawancara dilakukan secara semi terstruktur untuk menggali informasi mengenai potensi risiko kebocoran data dan upaya pencegahan yang diterapkan oleh rumah sakit. Analisis data menggunakan model Miles dan Huberman yang meliputi reduksi data, penyajian data, dan penarikan kesimpulan. Keabsahan data diuji melalui triangulasi sumber dan triangulasi metode dengan membandingkan hasil wawancara, observasi, dan dokumentasi untuk memastikan kesesuaian, konsistensi dan keakuratan data yang diperoleh selama penelitian. Penelitian ini memperhatikan aspek etika dengan menjaga kerahasiaan identitas informan serta memastikan bahwa data digunakan hanya untuk kepentingan penelitian.

Bagian ini memuat rancangan penelitian meliputi disain penelitian, populasi/ sampel penelitian, teknik dan instrumen pengumpulan data, alat analisis data, dan model penelitian yang digunakan. Metode yang sudah umum tidak perlu dituliskan secara rinci, tetapi cukup merujuk ke referensi acuan (misalnya: rumus uji-F, uji-t, dll). Pengujian validitas dan reliabilitas instrumen penelitian tidak perlu dituliskan secara rinci, tetapi cukup dengan

mengungkapkan hasil pengujian dan interpretasinya. Keterangan simbol pada model dituliskan dalam kalimat.

3. HASIL

Penelitian ini bertujuan untuk menganalisis risiko terjadinya kebocoran data pasien serta upaya pencegahan yang diterapkan dalam pengelolaan rekam medis elektronik di Rumah Sakit X. Hasil penelitian menunjukkan bahwa hingga saat penelitian dilakukan, belum ditemukan adanya laporan secara resmi mengenai insiden kebocoran data pasien. Namun, masih terdapat sejumlah kondisi yang berpotensi meningkatkan risiko kebocoran data, meliputi pemantauan *audit trail*, kebijakan hak akses yang belum sepenuhnya disesuaikan dengan peran da unit kerja pengguna, belum diterapkannya autentikasi dua faktor *(two-factor authentication)*, belum aktifnya kembali fitur *logout* otomatis *(idle time)*, penyimpanan *cloud* yang masih dalam tahap kajian, serta faktor *human error*. Kondisi tersebut menunjukkan perlu adanya pengawasan yang berkelanjutan dan penguatan pada sistem keamanan informasi.

Hak Akses dan Audit Trail

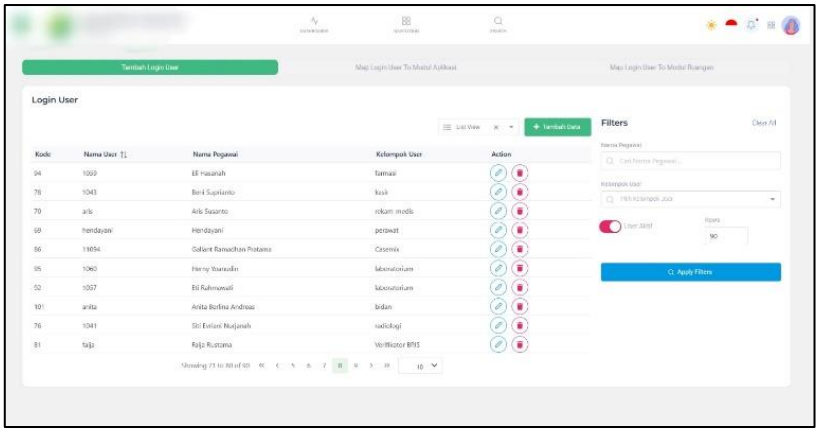
Berdasarkan hasil studi dokumentasi, pengaturan hak akses pengguna SIMRS di Rumah Sakit X telah ditetapkan melalui kebijakan yang mengatur pemberian hak akses sesuai kewenangan pengguna. Ringkasan pengaturan tersebut disajikan pada Tabel 2.

Tabel 2. Ringkasan Pengaturan Hak Akses Pengguna SIMRS Rumah Sakit X.

No	Jabatan/Unit Kerja	Hak Akses SIMRS	Batasan Kewenangan
1	Dokter / DPJP	*Read* & *Write* Data Medis	Menginput asmen, resep elektronik, order penunjang, melihat riwayat medis pasien sendiri
2	Perawat / Bidan	*Read* & *Write* Keperawatan	Menginput asuhan keperawatan, tanda-tanda vital, implementasi dokter.
3	Petugas Pendaftaran / Admisi	Read & *Write* Data Sosial	Menginput data demografi pasien, membuat kunjungan, tidak bisa melihat rekam medis.
4	Petugas Farmasi	*Read* Medis & *Write* Obat	Melihat resep dokter, melakukan skrining, menginput pengeluaran obat.
5	Manajemen / Direksi	*Read Only* (*Dashboard*/Laporan)	Melihat tren data, laporan capaian, statistik RS, tidak bisa mengubah data medis pasien.
6	Unit Rekam Medis (Koding/Indeksing)	*Read* & *Write* RM, Logistik RM	Melakukan koding diagnosa (ICD-10/9), retensi, dan manajemen berkas
7	Administrator IT	*Full Access* (Sistem)	Pemeliharaan sistem, manajemen *user*, tidak berhak mengubah isi rekam medis tanpa *log* audit.

Sumber: Kebijakan Hak Akses Internet dan Akses SIMRS RS X (2026)

Berdasarkan hasil observasi, akses ke SIMRS dilakukan menggunakan *username* dan *password* yang disesuaikan dengan hak akses setiap pengguna.



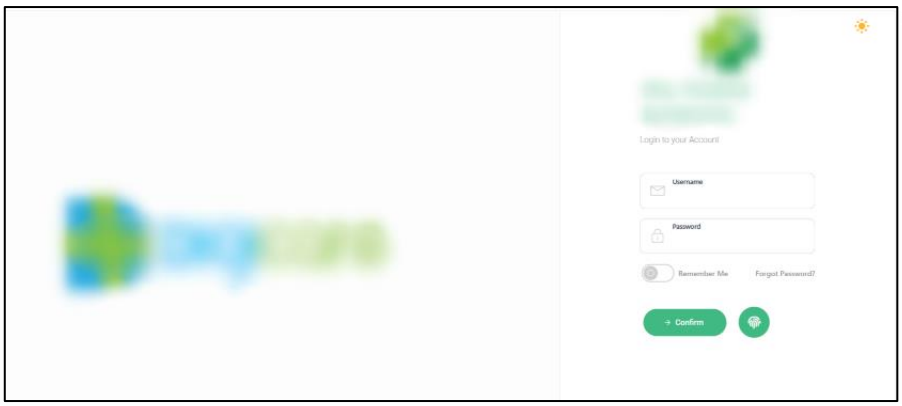
Gambar 1. Tampilan Hak Akses Pengguna.

Sumber: Diolah peneliti (2026)

Studi dokumentasi menunjukkan bahwa *audit trail* tidak mencatat penghapusan data medis secara ilegal selama periode evaluasi. Sementara itu, hasil wawancara menunjukkan bahwa pengaturan hak akses masih perlu dikembangkan sesuai dengan peran dan unit kerja pengguna.

Identifikasi dan Autentikasi Pengguna

Pengguna SIMRS melakukan *login* menggunakan *username* dan *password* pribadi sebelum memperoleh akses ke sistem. Proses tersebut ditampilkan pada Gambar 2.



Gambar 2. Tampilan Login SIMRS.

Sumber: Diolah peneliti (2026)

Hasil wawancara menunjukkan bahwa autentikasi masih menggunakan *username* dan *password*, sedangkan *two-factor authentication* (2FA) direncanakan untuk diterapkan secara bertahap sesuai *roadmap* pengembangan SIMRS.

Logout Otomatis *(Idle Time)*

Dokumen *monitoring* dan evaluasi rekam medis elektronik menunjukkan bahwa masih terdapat pengguna yang meninggalkan *workstation* tanpa *logout* sehingga akun tetap aktif. Ringkasan temuan disajikan pada Tabel 3.

Tabel 3. Temuan Terkait Logout Pengguna SIMRS.

No	Tanggal	Unit	Kronologis	Dampak
1	Tahun 2025	Tidak disebutkan	Ditemukan pengguna tidak melakukan *logout* setelah selesai menggunakan SIMRS sehingga akun masih aktif pada *workstation*. Selain itu, fitur *auto-lock* setelah 5 menit belum diterapkan.	Berpotensi menyebabkan penyalahgunaan akun oleh pengguna lain.

Sumber: Dokumen Monitoring dan Evaluasi RME Rumah Sakit X (2025)

Berdasarkan Tabel 3, masih ditemukan pengguna yang meninggalkan SIMRS tanpa melakukan *logout* sehingga akun tetap aktif pada *workstation*. Kondisi ini menunjukkan bahwa pengamanan sesi pengguna belum optimal dan masih membuka peluang penyalahgunaan akun oleh pihak lain.

Penyimpanan Data dan Server *Backup*

Rumah Sakit X menerapkan penyimpanan rekam medis elektronik melalui pemanfaatan server utama yang didukung oleh server *backup* lokal. Ringkasan hasil penelitian disajikan pada Tabel 4.

Tabel 4. Temuan Penyimpanan Data dan Server Backup**.**

No	Tanggal	Unit	Kronologis	Dampak
1	13 Maret 2026	Pendaftaran, rawat jalan, farmasi, kasir, dan poliklinik	Terjadi gangguan jaringan fiber optic yang mengakibatkan SIMRS mengalami *downtime* selama 187 menit. Selama gangguan berlangsung, pelayanan dilakukan secara manual. Selain itu, penyimpanan data RME belum didukung *cloud storage* sebagai media pencadangan tambahan.	Pencadangan data masih bergantung pada server *backup* lokal sehingga apabila terjadi gangguan pada infrastruktur penyimpanan, proses pemulihan data hanya mengandalkan media *backup* yang tersedia.

Sumber: Berita Acara Downtime SIMRS Rumah Sakit X (2026)

Berdasarkan Tabel 4, ketersediaan data RME masih bergantung pada sistem penyimpanan lokal yang digunakan rumah sakit. Belum tersedianya *cloud storage* sebagai media pencadangan tambahan menunjukkan bahwa penyimpanan data masih mengandalkan infrastruktur yang tersedia di rumah sakit.

Faktor *Human Error*

Berdasarkan hasil wawancara, ditemukan tindakan petugas yang berpotensi memicu kebocoran data pada rekam medis elektronik. Ringkasan temuan disajikan pada Tabel 5.

Tabel 5. Kronologi Potensi *Human Error.*

No	Tanggal	Unit	Kronologis	Dampak
1	Tidak tercatat	Rawat Jalan	Petugas memotret isi Catatan Perkembangan Pasien Terintegrasi (CPPT) dan mengirimkannya melalui media komunikasi untuk keperluan koordinasi pelayanan.	Berpotensi menyebabkan terbukanya informasi medis pasien kepada pihak yang tidak berwenang.

Sumber: Wawancara Kepala Instalasi Rekam Medis (2026)

4. PEMBAHASAN

Hak Akses dan Audit Trail

Hasil penelitian menunjukkan bahwa Rumah Sakit X telah menerapkan pengaturan hak akses pengguna SIMRS sesuai dengan kewenangan masing-masing. Namun, hasil wawancara mengungkapkan bahwa kebijakan tersebut masih memerlukan pengembangan karena belum mengatur hak akses secara rinci berdasarkan jabatan dan unit kerja. Selain, itu masih ditemukan permintaan akses dari beberapa unit yang tidak sesuai dengan ketentuan yang berlaku. Tim IT menjelaskan bahwa saat ini sedang dilakukan penyusunan ulang *Role-Based Access Control* (RBAC) melalui penyesuaian hak akses berdasarkan *job description* serta mekanisme persetujuan berjenjang sebelum hak akses diberikan. Kondisi ini menunjukkan perlunya penyempurnaan pengaturan hak akses berdasarkan tugas dan tanggung jawab setiap pengguna agar akses terhadap informasi hanya diberikan sesuai kebutuhan pekerjaan. Pengaturan yang belum spesifik dapat menyebabkan pengguna memperoleh hak akses yang melebihi kewenangan *(over privilege)*, sehingga meningkatkan risiko kebocoran data rekam medis elektonik. Temuan ini sejalan dengan penelitian yang menyatakan bahwa pengaturan hak akses berdasarkan tugas dan tanggung jawab pengguna berperan dalam membatasi akses tidak sah serta mengurangi risiko penyalahgunaan data rekam medis elektronik (Budiman et al., 2025).

Hasil penelitian juga menunjukkan bahwa selama periode evaluasi tidak ditemukan penghapusan data medis secara *ilegal* berdasarkan *audit trail*. Hal tersebut mengindikasikan bahwa aktivitas pengguna dalam SIMRS telah terekam sehingga dapat ditelusuri apabila terjadi dugaan penyalahgunaan sistem. Keterangan informan menunjukkan bahwa pemantauan audit trail secara berkala telah diusulkan kepada tim IT untuk memperkuat pengawasan keamanan sistem informasi sekaligus mendukung pemenuhan standar akreditasi rumah sakit. Hal tersebut sejalan dengan KMK No. HK0107-MENKES-1596-2024 tentang Standar Akreditasi pada MRMIK 2.1 dan MRMIK 2.2 yang mengatur penjaminan mutu melalui audit mutu terhadap sistem informasi rumah sakit, termasuk rekam medis elektronik, dengan pemantauan keamanan secara rutin. Regulasi tersebut juga memberikan contoh pemantauan terhadap pengguna yang melakukan perubahan pada rekam medis elektronik untuk memastikan penggunaan akses dan otorisasi telah diterapkan dengan tepat. Temuan ini sejalan dengan penelitian yang menyatakan bahwa audit trail akan lebih efektif apabila disertai *monitoring* dan evaluasi secara berkala sehingga setiap aktivitas yang berpotensi menimbulkan risiko keamanan dapat segera diidentifikasi dan ditindaklanjuti (Permana & Nuraeni, 2025). Oleh karena itu, pengembangan pengaturan hak akses serta optimalisasi pemantauan *audit trail* menjadi upaya penting dalam mengurangi risiko kebocoran data rekam medis elektronik di Rumah Sakit X.

Identifikasi dan Autentikasi Pengguna

Hasil penelitian menunjukkan bahwa pengguna SIMRS di Rumah Sakit X mengakses sistem menggunakan *username* dan *password* pribadi. Penerapan akun yang berbeda pada setiap pengguna menunjukkan bahwa rumah sakit telah menerapkan mekanisme identifikasi untuk mengendalikan akses terhadap rekam medis elektronik. Namun, autentikasi yang masih menggunakan *username* dan *password* menyebabkan keamanan akses bergantung pada kerahasiaan informasi *login* pengguna. Apabila informasi tersebut diketahui atau digunakan oleh pihak yang tidak berwenang, akun dapat disalahgunakan untuk mengakses data rekam medis elektronik tanpa izin. Kondisi ini berpotensi meningkatkan risiko pelanggaran kerahasiaan data pasien karena rekam medis elektronik memuat informasi kesehatan yang bersifat rahasia. Temuan ini sejalan dengan penelitian yang menyatakan bahwa autentikasi pengguna merupakan komponen penting dalam menjaga keamanan rekam medis elektronik sehingga setiap pengguna harus memiliki identitas akses yang jelas untuk mencegah penggunaan sistem oleh pihak yang tidak berwenang (Mahendra et al., 2025).

Hasil wawancara menunjukkan bahwa *two-factor authentication* (2FA) belum diterapkan di Rumah Sakit X dan telah masuk dalam *roadmap* pengembangan SIMRS untuk diimplementasikan secara bertahap. Kepala instalasi rekam medis menjelaskan bahwa proses autentikasi sebaiknya tidak hanya mengandalkan *password*, tetapi juga dilengkapi dengan faktor verifikasi tambahan, seperti kode verifikasi yang dikirim melalui email atau media lainnya. Kondisi tersebut menunjukkan adanya komitmen rumah sakit untuk memperkuat keamanan autentikasi sebagai bagian dari pelindungan data rekam medis elektronik. Temuan ini sejalan dengan penelitian yang menyatakan bahwa evaluasi keamanan rekam medis elektronik perlu mencakup aspek autentikasi pengguna sebagai salah satu bentuk pengendalian untuk meminimalkan risiko akses tidak sah terhadap data pasien (Apriliansyah, 2025).

Logout Otomatis *(Idle Time)*

Berdasarkan Tabel 3, hasil *monitoring* dan evaluasi rekam medis elektronik menunjukkan bahwa masih terdapat pengguna yang meninggalkan SIMRS tanpa melakukan *logout*. Kondisi tersebut menunjukkan bahwa pengamanan sesi pengguna masih bergantung pada kedisiplinan pengguna dalam mengakhiri akses ke sistem. Apabila *workstation* ditinggalkan saat akun masih aktif, pihak yang tidak berwenang berpotensi memanfaatkan akses tersebut sehingga meningkatkan risiko kebocoran data rekam medis elektronik. Temuan ini sejalan dengan penelitian yang menyatakan bahwa penerapan pengendalian keamanan pada rekam medis elektronik merupakan aspek penting dalam menjaga keamanan dan kerahasiaan data pasien (Mahendra et al., 2025)

Hasil wawancara dengan kepala instalasi rekam medis menunjukkan bahwa fitur *logout* otomatis pada SIMRS pernah diterapkan, tetapi dinonaktifkan karena menimbulkan *bug* yang menyebabkan pengguna harus *login* kembali ketika proses pelayanan masih berlangsung. Sementara itu, petugas IT menjelaskan bahwa fitur tersebut telah masuk dalam pengembangan SIMRS dan sedang melalui proses *debugging* agar sesi pengguna dapat berakhir secara otomatis setelah tidak ada aktivitas dalam jangka waktu tertentu tanpa mengganggu pelayanan. Temuan tersebut menunjukkan bahwa pelindungan sesi pengguna tidak hanya bergantung pada kebiasaan melakukan *logout* manual, tetapi juga memerlukan dukungan mekanisme keamanan sistem yang berjalan secara optimal.

Penyimpanan Data dan *Server Backup*

Berdasarkan Tabel 4, hasil penelitian menunjukkan bahwa penyimpanan rekam medis elektronik di Rumah Sakit X memanfaatkan server utama dan server *backup*. Kondisi tersebut menunjukkan bahwa rumah sakit telah menerapkan mekanisme pencadangan data untuk menjaga ketersediaan informasi apabila terjadi gangguan pada *server* utama. Namun, infrastruktur penyimpanan belum didukung oleh *cloud storage* sehingga belum sepenuhnya memenuhi standar akreditasi yang mensyaratkan keberadaan *server* utama, server *backup*, dan *cloud storage*. Temuan ini sejalan dengan penelitian yang menyatakan bahwa mekanisme penyimpanan dan pencadangan data merupakan aspek penting dalam menjaga keamanan serta keberlangsungan rekam medis elektronik apabila terjadi gangguan atau kehilangan data (Apriliansyah, 2025).

Hasil wawancara dengan petugas IT menunjukkan bahwa penyimpanan data saat ini masih menggunakan infrastruktur *on-premise* dengan sinkronisasi harian dari server utama ke server *backup*. Petugas IT juga menjelaskan bahwa penerapan *cloud storage* telah masuk dalam tahap kajian kelayakan dengan mempertimbangkan lokalisasi data serta rencana penggunaan *private cloud* tersertifikasi untuk menjaga kerahasiaan rekam medis elektronik. Apabila terjadi kerusakan sistem atau kehilangan data, pemulihan dilakukan melalui server *backup* menggunakan mekanisme data *recovery* dari *snapshot database* terakhir yang tersedia. Temuan tersebut menunjukkan bahwa mekanisme pencadangan data telah berjalan, tetapi pengembangan infrastruktur penyimpanan masih diperlukan untuk meningkatkan keamanan dan ketersediaan data rekam medis elektronik secara lebih optimal.

Faktor *Human Error*

Berdasarkan Tabel 5, hasil penelitian menunjukkan bahwa faktor *human error* masih menjadi salah satu potensi risiko kebocoran data rekam medis elektronik di Rumah Sakit X. Kondisi tersebut mengindikasikan bahwa pelindungan data pasien tidak hanya ditentukan oleh

penerapan teknologi keamanan, tetapi juga oleh kepatuhan pengguna terhadap prosedur keamanan informasi. Meskipun berbagai mekanisme pengamanan telah diterapkan, tindakan pengguna yang tidak sesuai dengan kebijakan tetap berpotensi mengakibatkan akses maupun penyebaran informasi pasien kepada pihak yang tidak berwenang. Temuan ini sejalan dengan penelitian yang menyatakan bahwa faktor manusia merupakan salah satu penyebab utama meningkatnya risiko keamanan rekam medis elektronik karena berkaitan dengan kepatuhan pengguna dalam menerapkan kebijakan dan prosedur keamanan informasi (Budiman et al., 2025).

Hasil wawancara dengan kepala instalasi rekam medis menunjukkan bahwa rumah sakit telah menyelenggarakan sosialisasi mengenai *cyber hygiene* dan *privacy security* sebagai upaya meningkatkan kesadaran petugas dalam menjaga kerahasiaan data pasien. Namun, masih ditemukan kejadian petugas memotret Catatan Perkembangan Pasien Terintegrasi (CPPT) dan mengirimkannya melalui grup rujukan untuk keperluan klarifikasi diagnosa. Walaupun dilakukan untuk mendukung proses pelayanan, penggunaan media komunikasi di luar sistem informasi rumah sakit tetap berpotensi meningkatkan risiko terbukanya informasi medis kepada pihak yang tidak berwenang apabila tidak disertai pengendalian yang memadai. Kejadian tersebut kemudian menjadi bahan evaluasi sehingga rumah sakit menetapkan kebijakan baru terkait penggunaan serta distribusi informasi pasien.

Upaya Pencegahan Kebocoran Rekam Medis Elektronik Pasien

Berdasarkan hasil penelitian, Rumah Sakit X telah menerapkan berbagai upaya pencegahan untuk mencegah kebocoran data rekam medis elektronik, antara lain melalui penggunaan akun *username* dan *password*, penerapan *firewall*, enkripsi basis data, *audit trail*, pembatasan akses ke ruang server, pencadangan data secara berkala, serta sosialisasi mengenai *cyber hygiene* dan *privacy security* kepada seluruh petugas. Selain pengendalian yang telah diterapkan, rumah sakit juga terus memperkuat keamanan sistem dengan melakukan penataan kembali *Role-Based Access Control* (RBAC) melalui penyesuaian hak akses berdasarkan *job description* dan penerapan mekanisme persetujuan berjenjang oleh kepala unit sebelum akses diberikan kepada pengguna. Pengembangan keamanan lainnya meliputi rencana implementasi *two-factor authentication* (2FA), pengaktifan kembali fitur *logout* otomatis setelah proses *debugging* selesai, penggunaan *private cloud* yang memenuhi ketentuan penyimpanan data, penerapan data *masking* untuk keperluan analisis maupun penelitian, serta peningkatan pemantauan keamanan sistem secara berkelanjutan.

5. KESIMPULAN

Berdasarkan hasil penelitian, hingga akhir pelaksanaan penelitian tidak ditemukan laporan resmi mengenai insiden kebocoran data rekam medis elektronik pasien di Rumah Sakit X. Namun, masih terdapat beberapa kondisi yang berpotensi meningkatkan risiko kebocoran data, meliputi belum dilakukannya pemantauan *audit trail* secara berkala sebagaimana ketentuan KMK No. HK0107-MENKES-1596-2024 tentang Standar Akreditasi pada MRMIK 2.1 dan MRMIK 2.2 yang mengatur pemantauan keamanan secara rutin serta pelacakan aktivitas pengguna pada rekam medis elektronik, pengaturan hak akses yang belum sepenuhnya disesuaikan dengan jabatan dan unit kerja, autentikasi yang masih mengandalkan *username* dan *password* tanpa penerapan *two-factor authentication* (2FA), fitur *logout* otomatis yang belum aktif kembali, penyimpanan data yang masih bergantung pada server *backup* tanpa dukungan *cloud storage*, serta faktor *human error*. Di sisi lain, rumah sakit telah menerapkan berbagai pengendalian teknis dan administratif serta terus melakukan penguatan terhadap sistem keamanan informasi.

Berdasarkan temuan penelitian, Rumah Sakit X disarankan memperkuat keamanan rekam medis elektronik melalui penataan *Role-Based Access Control* (RBAC) berdasarkan *job description* dan mekanisme persetujuan berjenjang sebelum pemberian hak akses, optimalisasi *monitoring audit trail* secara berkala, penerapan *two-factor authentication* (2FA), pengaktifan kembali fitur *logout* otomatis setelah proses *debugging*, implementasi *private cloud* sesuai ketentuan yang berlaku, serta peningkatan edukasi dan kepatuhan seluruh pengguna terhadap keamanan informasi. Upaya tersebut diharapkan dapat meminimalkan risiko kebocoran data sekaligus menjaga kerahasiaan, integritas, dan ketersediaan rekam medis elektronik pasien.

DAFTAR REFERENSI

Aldo Rizky Mahendra, Siswati Siswati, Dina Sonia, & Muhammad Fuad Iqbal. (2025). Tinjauan Sistem Keamanan Rekam Medis Elektronik di Rumah Sakit Al Dr. Mintohardjo Jakarta. *VitaMedica : Jurnal Rumpun Kesehatan Umum*, *3*(3), 73–85. https://doi.org/10.62027/vitamedica.v3i3.392

Apriliansyah, U. (2025). Evaluasi Manajemen Risiko Terkait Keamanan Data Rekam Medis Elektronik Di Rumah Sakit Mata Undaan Surabaya. *Jurnal Manajemen Kesehatan Yayasan RS.Dr. Soetomo*, *11*(2), 368–380. https://doi.org/10.29241/jmk.v11i2.2346

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

Fadli, M. R. (2021). Memahami Desain Metode Penelitian Kualitatif. *Humanika: Kajian Ilmiah Mata Kuliah Umum*, *21*(1), 33–54. https://doi.org/10.21831/hum.v21i1.38075

Fiantika, F. R., Wasil, M., Jumiyati, S., Honesti, L., Wahyuni, S., Mouw, E., Jonata, Mashudi, I., Hasanah, N., Maharani, A., Ambarwati, K., Noflidaputri, R., Nuryami, & Waris, L. (2022). *Metodologi Penelitian Kualitatif* (1st ed.). PT Global Eksekutif Teknologi.

Lestari, S., Sucipto, & Azizah, N. (2025). Tinjauan Penerapan Sistem Informasi Rekam Medis Elektronik Terhadap Keamanan Data Pasien di Rumah Sakit Kartini Rangkasbitung. *EDU RMIK Jurnal Edukasi Rekam Medis Informasi Kesehatan*, *4*(1), 43–56. https://doi.org/10.52031/erjermik.v4i1.975

Listyorini, P. I., & Sintya, I. (2021). SISTEM KEAMANAN SIMRS DI RUMAH SAKIT. *Prosiding Seminar Informasi Kesehatan Nasional (SIKesNas)*, 234–240. https://doi.org/10.47701/sikenas.v0i0.1257

Peraturan Menteri Kesehatan No. 24 Tahun 2022 Tentang Rekam Medis, Pub. L. No. 24 (2022). https://peraturan.bpk.go.id/Details/245544/permenkes-no-24-tahun-2022

Peraturan Presiden (Perpres) No. 18 Tahun 2020 Tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024, Pub. L. No. 18 (2020). https://peraturan.bpk.go.id/Details/131386/perpres-no-18-tahun-2020

Permana, O., & Nuraeni, Y. A. (2025). Evaluation of Data Security and Patient Confidentiality in the Electronic Medical Record System at Santosa Hospital Bandung Central. *Dinasti Health and Pharmacy Science*, *3*(1), 34–40. https://doi.org/10.38035/dhps.v3i1

Pradita, R., Kusumo, R., & Rahmawati. (2022). Pentingnya Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Puskesmas. *JOURNAL OF SUSTAINABLE COMMUNITY SERVICE*, *2*(2), 52–62. https://doi.org/10.55047/jscs.v2i2.437

Putra, F. F., & Widyaningrum, D. (2025). Pengaruh Penerapan Rekam Medis Elektronik Terhadap Efektivitas Pelayanan Rawat Jalan RSUD Kesehatan Kerja Provinsi Jawa Barat. *Jurnal Riset Sains Dan Kesehatan Indonesia*, *2*(6), 263–271. https://doi.org/10.69930/jrski.v2i6.624

Sorisa, C., Kiareni, C. L., & Parhusip, J. (2024). Etika Keamanan Siber : Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia. *Jurnal Sains Student Research*, *2*(6), 586–593. https://doi.org/10.61722/jssr.v2i6.2996

Sugiyono. (2019). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (2nd ed.). Alfabeta.

Suhariyono, U. S., Ikawati, F. R., & Afifah, N. (2025). Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso. *Jurnal Manajemen Informasi Kesehatan Indonesia*, *13*(1), 72–78. https://doi.org/10.33560/jmiki.v13i1.812

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

Undang-Undang No. 17 Tahun 2023 Tentang Kesehatan, Pub. L. No. 17 (2023). https://peraturan.bpk.go.id/details/258028/uu-no-17-tahun-2023

Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Pub. L. No. 27 (2022). https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022