NURSING CARE AND HEALTH TECHNOLOGY
http://ojs.nchat.id/index.php/nchat

Manajemen Risiko Pengamanan Data Pasien Dalam E-Rekam Medis di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara

Edy Husnul Mujahid[1*], Acep Rohendi[2], Yani Restiani Widjaja[3], Erliany Syaodih[4], I Putu Sudayasa[5], Putu Agustin Kusumawati[6]

[1,2,3,4] Manajemen Rumah Sakit, Fakultas Ekonomi dan Bisnis, Universitas Adhirajasa Reswara Sanjaya Bandung, Indonesia

[5] Departemen Kedokteran Komunitas, Fakultas Kedokteran, Universitas Halu Oleo, Kendari, Indonesia

[6] Rumah Sakit Jiwa Provinsi Sulawesi Tenggara, Kendari, Indonesia

ABSTRAK

Transformasi digital dalam sistem pelayanan kesehatan telah mendorong adopsi e-rekam medis (EMR) untuk meningkatkan efisiensi dan kualitas pelayanan. Namun, implementasi EMR menghadirkan tantangan baru terkait pengamanan data pasien, khususnya di rumah sakit jiwa yang menangani informasi sangat sensitif. Penelitian ini bertujuan untuk mendeskripsikan implementasi manajemen risiko pengamanan data pasien dalam e-rekam medis di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara, serta mengidentifikasi kendala dan strategi mitigasi yang diterapkan. Penelitian menggunakan pendekatan kualitatif dengan metode studi kasus. Teknik pengumpulan data meliputi wawancara mendalam, observasi, dan studi dokumentasi, dengan analisis tematik terhadap data yang diperoleh. Hasil penelitian menunjukkan bahwa meskipun kebijakan dan prosedur keamanan informasi telah disusun, pelaksanaannya belum berjalan optimal. Hambatan utama yang dihadapi antara lain keterbatasan pemahaman staf, infrastruktur teknologi yang belum memadai, serta lemahnya budaya organisasi dalam mendukung perlindungan data pasien. Strategi mitigasi seperti pembentukan tim IT dan pelatihan internal telah dilakukan namun masih bersifat terbatas. Kesimpulan penelitian bahwa implementasi manajemen risiko pengamanan data pasien dalam sistem e-rekam medis di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara masih belum berjalan secara optimal. Rumah sakit telah memiliki kebijakan dan prosedur dasar mengenai keamanan informasi, namun pelaksanaannya masih belum merata di seluruh unit layanan.

Kata kunci: E-Rekam Medis, Informasi Pasien, Keamanan Data, Manajemen Risiko, Rumah Sakit Jiwa

ABSTRACT

The digital transformation in healthcare services has encouraged the adoption of electronic medical records (EMRs) to improve efficiency and service quality. However, EMR implementation presents new challenges in securing patient data, especially in psychiatric hospitals where information is highly sensitive. This study aims to describe the implementation of risk management for patient data security in EMRs at the Psychiatric Hospital of Southeast Sulawesi Province and to identify the key challenges and mitigation strategies applied. A qualitative approach with a case study method was used. Data were collected through in-depth interviews, direct observation, and document analysis, and analyzed thematically. The findings reveal that although data security policies and procedures have been established, their implementation remains suboptimal. The main obstacles include limited staff understanding, inadequate technological infrastructure, and a weak organizational culture in supporting patient data protection. Mitigation efforts such as forming an IT team and conducting internal training have been initiated but remain limited in scope. The study concluded that the implementation of patient data security risk management in the e-medical records system at the Southeast Sulawesi Provincial Mental Hospital is still not optimal. The hospital has basic policies and procedures regarding information security, but their implementation is still uneven across all service units.

Keywords: *E-Medical Records, Patient Information, Data Security, Risk Management, Mental Hospitals*

Koresponden:
Nama : Edy Husnul Mujahid
Alamat : Kampus Hijau Bumi Tridharma, Anduonohu, Kec. Kambu, Kota Kendari, Sulawesi Tenggara
No. Hp : +62 813-4257-7717
e-mail : edy.husnul@uho.ac.id

Received 29 Agustus 2025 • Accepted 5 Oktober 2025 • Published 12 Oktober 2025
e - ISSN : 2798-107X • DOI: https://doi.org/10.56742/nchat.v5i2.215

PENDAHULUAN

Transformasi digital di sektor kesehatan telah mendorong adopsi sistem informasi elektronik, termasuk penerapan *electronic medical records* (EMR) atau *e-rekam medis*. Sistem ini dirancang untuk menyimpan data kesehatan pasien secara digital, mulai dari identitas, riwayat penyakit, hasil pemeriksaan, hingga pengobatan. Digitalisasi ini tidak hanya bertujuan untuk meningkatkan efisiensi, akurasi pencatatan, dan kemudahan akses data oleh tenaga kesehatan, tetapi juga menjadi prasyarat untuk menghadapi era layanan kesehatan berbasis teknologi [1,2]. Pemerintah Indonesia, melalui Peraturan Menteri Kesehatan Nomor 24 Tahun 2022, mewajibkan seluruh fasilitas pelayanan kesehatan untuk mengimplementasikan rekam medis elektronik sebagai bagian dari sistem pelayanan terstandar dan terintegrasi [3].

Namun, seiring dengan meningkatnya penggunaan sistem digital dalam penyimpanan data pasien, isu mengenai keamanan dan kerahasiaan informasi menjadi semakin krusial. Data pasien, terutama data kesehatan mental, merupakan informasi pribadi yang sangat sensitif dan memiliki risiko tinggi terhadap penyalahgunaan apabila tidak dilindungi dengan baik. Kebocoran data dapat menimbulkan dampak serius, seperti hilangnya kepercayaan pasien, diskriminasi sosial, hingga konsekuensi hukum bagi institusi penyedia layanan [4]. Oleh karena itu, sistem keamanan informasi dalam pengelolaan *e-rekam medis* perlu dirancang dan diterapkan secara menyeluruh melalui pendekatan manajemen risiko yang berbasis standar internasional dan regulasi nasional [5].

Rumah Sakit Jiwa Provinsi Sulawesi Tenggara sebagai institusi pelayanan kesehatan mental di Indonesia menghadapi tantangan kompleks dalam implementasi *e-rekam medis*. Selain beban administratif dan keterbatasan infrastruktur, rumah sakit ini juga harus menangani karakteristik unik data pasien jiwa yang lebih sensitif dibandingkan pasien umum [6]. Stigma sosial terhadap gangguan mental membuat perlindungan terhadap privasi informasi menjadi isu utama yang tidak bisa diabaikan. Dalam konteks ini, pendekatan terhadap manajemen risiko tidak hanya berorientasi pada aspek teknis, tetapi juga melibatkan dimensi etika, hukum, serta budaya organisasi [7].

Manajemen risiko keamanan data adalah proses sistematis yang mencakup identifikasi, analisis, evaluasi, serta mitigasi terhadap berbagai potensi ancaman terhadap sistem informasi. Standar internasional seperti ISO/IEC 27001 dan ISO 27799, serta kerangka nasional seperti Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), memberikan landasan yuridis dan teknis yang kuat bagi rumah sakit untuk menyusun kebijakan keamanan informasi yang terintegrasi. Dalam implementasinya, proses manajemen risiko harus memperhitungkan berbagai faktor seperti kesalahan manusia, kelemahan sistem, ancaman internal, serta serangan siber dari pihak luar [2,8].

Faktanya, implementasi sistem keamanan data dalam *e-rekam medis* di RS Jiwa Provinsi Sulawesi Tenggara belum berjalan optimal. Temuan awal menunjukkan masih adanya ketimpangan antara kebijakan yang berlaku dengan praktik di lapangan. Rendahnya tingkat pelatihan dan kesadaran staf terhadap pentingnya menjaga kerahasiaan data, keterbatasan infrastruktur teknologi, serta lemahnya budaya organisasi dalam mendukung tata kelola keamanan informasi menjadi faktor penyebab utama. Dalam beberapa kasus, bahkan ditemukan potensi kerentanan terhadap akses tidak sah dan kebocoran data akibat lemahnya sistem kontrol dan pengawasan.

Masalah riil yang muncul adalah adanya kesenjangan antara kebijakan formal yang sudah disusun dengan praktik di lapangan. Banyak staf belum memahami prinsip dasar keamanan data, infrastruktur TI yang tersedia masih minim (tanpa sistem enkripsi menyeluruh, firewall, atau deteksi intrusi), serta belum terbentuk budaya organisasi yang mendukung perlindungan informasi pasien secara konsisten. Kondisi ini menimbulkan kerentanan serius, misalnya potensi akses tidak sah ke data rekam medis, lemahnya kontrol pengguna, hingga tidak adanya mekanisme audit risiko yang jelas. Jika tidak ditangani, situasi ini dapat meningkatkan risiko kebocoran data yang merugikan pasien maupun rumah sakit.

Urgensi studi ini terletak pada tingginya sensitivitas data pasien jiwa. Informasi terkait riwayat terapi, catatan psikiatri, hingga penggunaan obat psikotropika bukan hanya berdampak klinis, tetapi juga berimplikasi

pada aspek sosial dan psikologis pasien. Pelanggaran kerahasiaan dapat memicu stigma, diskriminasi, bahkan mengganggu proses pemulihan pasien. Selain itu, meningkatnya ancaman siber di sektor kesehatan menjadikan rumah sakit jiwa rentan terhadap serangan digital jika tidak memiliki sistem manajemen risiko yang memadai.

Penelitian ini bertujuan untuk mendeskripsikan bagaimana implementasi manajemen risiko pengamanan data pasien dalam *e-rekam medis* di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara. Penelitian ini juga akan mengidentifikasi kendala-kendala utama yang dihadapi oleh rumah sakit dalam penerapan sistem keamanan informasi, serta menganalisis upaya-upaya mitigasi yang telah dan sedang dilakukan.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif, yang bertujuan untuk menggambarkan secara mendalam dan komprehensif tentang implementasi manajemen risiko pengamanan data pasien dalam sistem e-rekam medis di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara. Pendekatan ini dipilih karena memungkinkan peneliti untuk memahami secara kontekstual fenomena yang kompleks dalam setting alami, terutama menyangkut kebijakan, praktik pengamanan data, serta persepsi dan pengalaman para pelaku sistem informasi kesehatan di rumah sakit tersebut. Studi kasus juga relevan digunakan karena fokus penelitian diarahkan pada satu institusi secara spesifik yang memiliki karakteristik unik, yaitu rumah sakit jiwa dengan konteks data pasien yang sensitif dan berisiko tinggi.

Penelitian ini dilaksanakan di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara selama periode Mei hingga Juli 2025. Lokasi penelitian dipilih secara purposive karena rumah sakit ini telah menerapkan sistem e-rekam medis namun menghadapi tantangan signifikan dalam aspek pengamanan data pasien. Waktu pelaksanaan penelitian disesuaikan secara fleksibel berdasarkan jadwal informan dan izin institusi, guna memastikan proses pengumpulan data berjalan efektif tanpa mengganggu aktivitas layanan rumah sakit.

Subjek penelitian terdiri atas informan yang dipilih secara purposive berdasarkan keterlibatan langsung mereka dalam proses manajemen sistem informasi rumah sakit dan pengelolaan data pasien. Informan tersebut meliputi kepala instalasi rekam medis, tim teknologi informasi (IT), manajemen rumah sakit, tenaga medis (dokter, perawat, dan psikolog), serta bagian hukum dan tata kelola. Kriteria pemilihan informan mencakup pengetahuan, pengalaman, dan peran mereka dalam implementasi serta pengawasan keamanan informasi di rumah sakit. Jumlah informan ditentukan dengan pendekatan data saturation, yaitu ketika informasi yang diperoleh telah menunjukkan pola yang konsisten dan tidak menghasilkan temuan baru yang signifikan.

Teknik pengumpulan data dalam penelitian ini terdiri dari tiga metode utama, yaitu wawancara mendalam, observasi langsung, dan studi dokumentasi. Wawancara dilakukan secara semi-terstruktur dengan panduan pertanyaan yang fleksibel agar dapat mengeksplorasi pengalaman dan pandangan informan secara terbuka. Observasi dilakukan untuk mengamati secara langsung interaksi staf dalam penggunaan sistem e-rekam medis serta penerapan kebijakan pengamanan data di lingkungan kerja mereka. Studi dokumentasi mencakup penelaahan terhadap dokumen kebijakan rumah sakit, standar operasional prosedur (SOP), laporan insiden keamanan informasi (jika tersedia), dan dokumen lain yang relevan dengan sistem keamanan data dan manajemen risiko.

Data yang diperoleh dianalisis menggunakan pendekatan analisis tematik. Langkah pertama adalah transkripsi data hasil wawancara, dilanjutkan dengan pembacaan berulang untuk mengenali tema awal dan mengidentifikasi isu utama yang muncul dari narasi informan. Proses pengkodean terbuka dan aksial kemudian dilakukan untuk mengelompokkan data ke dalam kategori tematik berdasarkan prinsip-prinsip manajemen risiko, seperti identifikasi risiko, analisis risiko, evaluasi risiko, dan mitigasi risiko. Selanjutnya, peneliti menyusun narasi tematik berdasarkan hubungan antara kategori yang terbentuk dan konteks situasional rumah sakit. Validasi dilakukan melalui triangulasi antar sumber data, pengecekan ulang kepada informan (member check), dan refleksi kritis oleh peneliti.

Keabsahan data dijaga melalui penerapan prinsip trustworthiness sebagaimana dikembangkan oleh Lincoln dan Guba, yang mencakup empat aspek, yaitu credibility, transferability, dependability, dan confirmability. Kredibilitas data diperoleh melalui triangulasi teknik dan konfirmasi ulang kepada informan. Transferabilitas dijaga melalui deskripsi kontekstual yang rinci. Dependabilitas dicapai dengan dokumentasi proses yang sistematis dan transparan, sementara confirmability dilakukan dengan menjaga jarak interpretasi subjektif dan memelihara audit trail selama proses penelitian.

Aspek etika penelitian menjadi bagian penting dalam pelaksanaan studi ini. Seluruh partisipan diberikan penjelasan mengenai tujuan dan manfaat penelitian serta menandatangani informed consent sebelum wawancara dimulai. Identitas informan dijaga kerahasiaannya dengan menggunakan kode tertentu, dan data yang dikumpulkan tidak akan digunakan di luar kepentingan akademik. Peneliti juga telah memperoleh izin resmi dari manajemen Rumah Sakit Jiwa Provinsi Sulawesi Tenggara sebelum melakukan kegiatan penelitian. Seluruh proses dilakukan dengan menjunjung tinggi prinsip netralitas, transparansi, dan akuntabilitas demi menjaga integritas ilmiah dan perlindungan terhadap hak-hak subjek penelitian.

HASIL

Penelitian ini bertujuan untuk mendeskripsikan implementasi manajemen risiko pengamanan data pasien dalam e-rekam medis di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara. Berdasarkan hasil wawancara mendalam, observasi lapangan, dan studi dokumentasi, diperoleh temuan utama yang mencerminkan tiga aspek penting dalam pelaksanaan manajemen risiko, yaitu: (1) pelaksanaan kebijakan pengamanan data, (2) hambatan dalam implementasi manajemen risiko, dan (3) strategi mitigasi yang diterapkan rumah sakit dalam menghadapi tantangan keamanan data.

Hasil temuan menunjukkan bahwa secara formal, rumah sakit telah memiliki dokumen kebijakan dan prosedur standar operasional (SOP) terkait pengelolaan e-rekam medis dan pengamanan data pasien. Sistem e-rekam medis telah diterapkan dan mencakup fitur akses berbasis akun pengguna, pencatatan aktivitas pengguna (audit trail), serta sistem pencadangan (backup) data secara periodik. Namun, pelaksanaan kebijakan tersebut belum berjalan optimal di semua unit. Beberapa petugas medis masih mencatat data secara manual sebagai bentuk antisipasi terhadap ketidakstabilan sistem, dan sebagian staf belum sepenuhnya memahami prosedur standar pengamanan data, terutama yang berkaitan dengan kerahasiaan, integritas, dan otorisasi akses data pasien.

Dari sisi sumber daya manusia, keterbatasan kapasitas dan pemahaman staf menjadi salah satu kendala utama. Hasil wawancara menunjukkan bahwa belum semua tenaga kesehatan menerima pelatihan formal mengenai keamanan informasi atau prinsip dasar manajemen risiko data. Beberapa staf bahkan tidak menyadari risiko pelanggaran data yang dapat timbul dari praktik sehari-hari, seperti tidak mengunci komputer saat meninggalkan meja kerja atau berbagi akun pengguna. Kesadaran terhadap kerahasiaan data pasien, khususnya pasien jiwa yang memiliki tingkat sensitivitas tinggi, belum tertanam secara merata di lingkungan kerja rumah sakit.

Selain itu, rumah sakit menghadapi keterbatasan infrastruktur teknologi. Kapasitas server dan perangkat lunak yang digunakan masih bersifat dasar dan belum mendukung sistem deteksi intrusi atau enkripsi data secara menyeluruh. Jaringan internal belum dilengkapi dengan firewall atau sistem keamanan canggih, sehingga rentan terhadap gangguan teknis dan potensi serangan siber. Tidak adanya tim keamanan informasi yang khusus menangani insiden data juga menjadi salah satu celah dalam sistem perlindungan data rumah sakit.

Dalam menghadapi berbagai tantangan tersebut, rumah sakit telah melakukan beberapa upaya mitigasi. Tim IT rumah sakit menjadi ujung tombak dalam pengelolaan dan pemeliharaan sistem e-rekam medis, termasuk dalam hal pemantauan dan pemulihan data. Upaya pelatihan internal secara terbatas telah dilakukan untuk staf bagian rekam medis dan beberapa tenaga kesehatan, meskipun belum menyeluruh dan berkelanjutan.

Rumah sakit juga mulai menyusun kebijakan internal yang merujuk pada regulasi nasional, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis.

Namun demikian, hasil penelitian menunjukkan bahwa pengelolaan risiko keamanan data di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara masih berada dalam tahap awal. Belum terdapat sistem audit risiko secara berkala, belum ada prosedur penanganan insiden keamanan data yang terdokumentasi, serta belum terbentuk budaya organisasi yang kuat dalam mendukung keamanan informasi. Sistem keamanan lebih bersifat reaktif daripada proaktif, dan pelaporan insiden belum diformalkan dalam bentuk laporan tertulis atau evaluasi sistematis.

Penelitian ini hanya berfokus pada Rumah Sakit Jiwa Provinsi Sulawesi Tenggara. Hal ini membuat temuan sulit digeneralisasi untuk seluruh rumah sakit jiwa di Indonesia maupun fasilitas kesehatan lain dengan kondisi berbeda. Kedua, penggunaan metode kualitatif memberikan pemahaman yang mendalam, tetapi tidak menyertakan data kuantitatif (misalnya tingkat kepatuhan staf atau jumlah insiden pelanggaran data). Akibatnya, sulit mengukur sejauh mana tingkat risiko secara objektif.

Dengan demikian, dapat disimpulkan bahwa implementasi manajemen risiko pengamanan data pasien dalam e-rekam medis di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara masih bersifat parsial dan belum terintegrasi dalam sistem tata kelola informasi rumah sakit secara komprehensif. Diperlukan peningkatan kapasitas SDM melalui pelatihan berkelanjutan, penguatan infrastruktur TI, pembentukan unit khusus keamanan data, serta pengembangan kebijakan dan prosedur yang lebih sistematis dan sesuai standar. Upaya ini penting untuk memastikan bahwa perlindungan data pasien, khususnya pasien jiwa, dapat dilaksanakan secara konsisten, profesional, dan akuntabel.

PEMBAHASAN

Hasil penelitian menunjukkan bahwa implementasi manajemen risiko pengamanan data pasien dalam sistem e-rekam medis di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara belum sepenuhnya optimal. Temuan ini sejalan dengan konsep manajemen risiko menurut ISO 31000, yang menekankan pentingnya integrasi antara proses identifikasi risiko, analisis, evaluasi, serta tindakan mitigasi sebagai satu kesatuan yang berkesinambungan dalam kerangka tata kelola organisasi [7]. Dalam konteks rumah sakit, khususnya rumah sakit jiwa, proses tersebut menjadi semakin penting karena data yang dikelola bersifat sangat sensitif dan berdampak langsung terhadap aspek psikososial pasien jika terjadi pelanggaran privasi [5].

Kelemahan utama dalam implementasi manajemen risiko di rumah sakit ini ditemukan pada tiga aspek: sumber daya manusia, infrastruktur teknologi, dan budaya organisasi. Dari sisi sumber daya manusia, rendahnya pemahaman dan kesadaran staf terhadap prinsip-prinsip keamanan data mencerminkan belum terbangunnya sistem pelatihan yang terstruktur. Hal ini mendukung pendapat Hossid et al., [9], yang menyatakan bahwa kesadaran staf merupakan determinan utama dalam keberhasilan pengelolaan keamanan informasi di sektor kesehatan. Selain itu, hasil penelitian ini mengonfirmasi temuan Basil et al. [10], bahwa kegagalan dalam membangun pemahaman kolektif terhadap ancaman digital menjadi salah satu faktor risiko terbesar dalam sistem e-health.

Dari sisi teknologi, keterbatasan perangkat keras, minimnya sistem proteksi seperti firewall dan sistem deteksi intrusi (IDS), serta tidak adanya enkripsi data yang menyeluruh, mengindikasikan belum terpenuhinya standar minimum sistem manajemen keamanan informasi sebagaimana tercantum dalam ISO/IEC 27001 dan ISO 27799. Hal ini selaras dengan hasil studi sardi et al., [11], yang menyatakan bahwa keamanan data pasien bergantung pada penerapan kontrol teknis yang ketat, termasuk autentikasi, otorisasi, dan pelacakan aktivitas pengguna. Dalam konteks rumah sakit jiwa, risiko ini diperburuk oleh fakta bahwa data yang dikelola mencakup

catatan terapi, riwayat psikiatri, dan penggunaan obat psikotropika, yang memiliki potensi tinggi untuk disalahgunakan bila jatuh ke tangan yang tidak berwenang [12].

Budaya organisasi yang belum mendukung praktik keamanan informasi juga menjadi hambatan signifikan. Hasil observasi dan wawancara mengindikasikan bahwa sebagian besar staf belum menginternalisasi pentingnya keamanan data sebagai bagian dari tanggung jawab profesional mereka. Hal ini memperkuat argumen Yuliana dan Hartono [13], yang menyebutkan bahwa transformasi budaya organisasi menjadi fondasi penting dalam menciptakan sistem informasi yang aman dan berkelanjutan. Dalam lingkungan rumah sakit jiwa, budaya organisasi harus secara aktif membangun nilai-nilai kepercayaan, etika, dan akuntabilitas dalam perlindungan hak privasi pasien.

Dari segi kebijakan, Rumah Sakit Jiwa Provinsi Sulawesi Tenggara telah mengacu pada Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Namun, penelitian ini menunjukkan adanya gap antara kebijakan formal dan praktik di lapangan. Hal ini senada dengan temuan penelitian Usman et al. [14], yang menyatakan bahwa keberadaan regulasi tidak serta-merta menjamin kepatuhan, terutama jika tidak didukung oleh sistem internal yang kuat dan mekanisme monitoring yang jelas. Dalam hal ini, rumah sakit perlu menyesuaikan prosedur internal dengan prinsip-prinsip dasar yang digariskan dalam peraturan nasional maupun standar internasional .

Upaya mitigasi yang telah dilakukan, seperti pelatihan dasar, pembentukan tim IT, serta pengembangan SOP internal, merupakan langkah awal yang positif. Namun, upaya tersebut belum cukup untuk menciptakan sistem pengelolaan risiko yang proaktif dan adaptif terhadap perkembangan ancaman digital [15]. Diperlukan pendekatan yang lebih sistematis dan menyeluruh, termasuk penguatan sistem audit internal, integrasi manajemen risiko ke dalam struktur organisasi, dan pemanfaatan teknologi keamanan informasi berbasis *real-time monitoring*. Strategi ini sejalan dengan prinsip CIA Triad (Confidentiality, Integrity, Availability), yang menjadi kerangka utama dalam desain sistem keamanan data di sektor kesehatan [5].

Dengan demikian, penelitian ini menegaskan bahwa pengelolaan risiko keamanan data dalam e-rekam medis di rumah sakit jiwa tidak dapat disamakan dengan rumah sakit umum. Keunikan data pasien jiwa, risiko diskriminasi sosial, dan beban etik yang tinggi menuntut perhatian khusus dan perlindungan yang lebih kuat. Oleh karena itu, implementasi manajemen risiko pengamanan data harus menjadi bagian integral dari sistem tata kelola rumah sakit, yang melibatkan semua komponen: manajemen, teknologi, sumber daya manusia, dan budaya organisasi.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa implementasi manajemen risiko pengamanan data pasien dalam sistem e-rekam medis di Rumah Sakit Jiwa Provinsi Sulawesi Tenggara masih belum berjalan secara optimal. Rumah sakit telah memiliki kebijakan dan prosedur dasar mengenai keamanan informasi, namun pelaksanaannya masih belum merata di seluruh unit layanan. Beberapa faktor yang menjadi kendala dalam penerapan manajemen risiko antara lain rendahnya pemahaman staf terhadap prinsip keamanan data, terbatasnya pelatihan terkait, kurangnya infrastruktur teknologi yang memadai, serta lemahnya sistem pengawasan dan evaluasi terhadap kebijakan yang telah ditetapkan. Upaya mitigasi yang telah dilakukan, seperti pembentukan tim IT dan sosialisasi SOP, masih bersifat parsial dan belum membentuk sistem yang berkelanjutan. Oleh karena itu, pengelolaan risiko keamanan informasi di rumah sakit ini masih perlu ditingkatkan guna memastikan perlindungan data pasien, khususnya pasien jiwa, yang memiliki tingkat kerahasiaan tinggi.

Berdasarkan temuan tersebut, peneliti memberikan beberapa saran yang dapat dijadikan bahan pertimbangan dalam perbaikan sistem. Pertama, rumah sakit perlu meningkatkan kapasitas sumber daya manusia melalui pelatihan rutin dan sosialisasi tentang pentingnya keamanan data dan kerahasiaan informasi

pasien. Kedua, perlu dilakukan penguatan infrastruktur teknologi, khususnya dalam hal keamanan jaringan, sistem backup data, dan penggunaan teknologi enkripsi. Ketiga, manajemen rumah sakit disarankan untuk membentuk unit atau tim khusus yang fokus menangani keamanan informasi, termasuk melakukan pemantauan dan evaluasi secara berkala. Keempat, audit internal terhadap implementasi SOP dan sistem keamanan data perlu dilakukan secara rutin untuk mengidentifikasi dan memperbaiki celah yang ada. Terakhir, disarankan agar penelitian serupa dilakukan di rumah sakit lain dengan karakteristik berbeda agar diperoleh gambaran yang lebih luas dan komprehensif mengenai praktik manajemen risiko pengamanan data pasien di fasilitas layanan kesehatan di Indonesia.

DAFTAR PUSTAKA

1. Abernethy A, Adams L, Barrett M, Bechtel C, Brennan P, Butte A, et al. The promise of digital health: then, now, and the future. NAM Perspect. 2022;2022:10–31478. [View at Publisher] [Google Scholar]
2. Ahmad A, Hastuti J, Hijriatin M. Data Security Analysis in Electronic Health Information Systems. J Informatic, Educ Manag. 2025;7(1):1–11. [View at Publisher] [Google Scholar]
3. Asgiani, Suryawati A. A literature review: Security Aspects in the Implementation of Electronic Medical Records in Hospitals. Media Ilmu Kesehat. 2021;10(2). [View at Publisher] [Google Scholar]
4. Mandey AW. Legal Analysis of Patient Privacy Violation in Electronic Medical Records and its Implications for Health Data Protection in Indonesia. J Multidisiplin Sahombu. 2025;5(02):589–94. [View at Publisher] [Google Scholar]
5. Larasati T, Fardiansyah AI, Saketi D, Dewiarti AN. The Ethical and Legal Aspects of Health Policy on Electronic Medical Records in Indonesia. Cepalo. 2024;8(2):103–12. [View at Publisher] [Google Scholar]
6. Shojaei P, Vlahu-Gjorgievska E, Chow YW. Security and privacy of technologies in health information systems: A systematic literature review. Computers. 2024;13(2):41. [View at Publisher] [Google Scholar]
7. Sari PK, Handayani PW, Hidayanto AN, Yazid S, Aji RF. Information security behavior in health information systems: a review of research trends and antecedent factors. In: Healthcare. MDPI; 2022. p. 2531. [View at Publisher] [Google Scholar]
8. Akhmad TR, Pranadita N, Machmud S. Legal Protection Of Patients From Leakage Of Electronic Medical Records Data Is Reviewed From Law Number 27 Of 2022 Concerning Personal Data Protection And Law Number 17 Of 2023 Concerning Health. Int J Asia Pasific Collab. 2024;2(3). [Google Scholar]
9. Hossain MK, Sutanto J, Handayani PW, Haryanto AA, Bhowmik J, Frings-Hessami V. An exploratory study of electronic medical record implementation and recordkeeping culture: the case of hospitals in Indonesia. BMC Health Serv Res. 2025;25(1):1–20. [View at Publisher] [Google Scholar]
10. Basil NN, Ambe S, Ekhator C, Fonkem E, Nduma BN. Health records database and inherent security concerns: A review of the literature. Cureus. 2022;14(10). [View at Publisher] [Google Scholar]
11. Sardi A, Rizzi A, Sorano E, Guerrieri A. Cyber risk in health facilities: A systematic literature review. Sustainability. 2020;12(17):7002. [View at Publisher] [Google Scholar]
12. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egypt Informatics J. 2021;22(2):177–83. [View at Publisher] [Google Scholar]
13. Firdaus R, Syeira K, Wijaya N. Transformasi Digital Sistem Informasi Kesehatan Menuju Layanan Kesehatan Yang Terkoneksi Dan Berpusat Pada Pasien. Econ Digit Bus Rev. 2025;6(2):1045–55. [View at Publisher] [Google Scholar]
14. Usman M, Qamar U. Secure electronic medical records storage and sharing using blockchain technology. Procedia Comput Sci. 2020;174:321–7. [View at Publisher] [Google Scholar]

15. Wu Z, Xuan S, Xie J, Lin C, Lu C. How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective. Comput Biol Med. 2022;147:105726. [View at Publisher] [Google Scholar]